MPSI
PCSI

1re ANNÉE

Conforme aux programmes

ANALYSE

COURS
EXERCICES CORRIGÉS

2e édition

GILLES COSTANTINI

de boeck supérieur

ANALYSE

Collection Prépas Scientifiques
Dirigée par Olivier Rodot

ANTONINI C., Algèbre. 2e année

BASBOIS N. et ABBRUGIATI P., Algèbre. 1re année, 2e édition

COSTANTINI G., Analyse. 1re année, 2e édition

DAO DUC K. et DELAUNAY D., Probabilités

JAN C., Mathématiques. Une approche imagée et synthétique. 1re année, 2e éd.

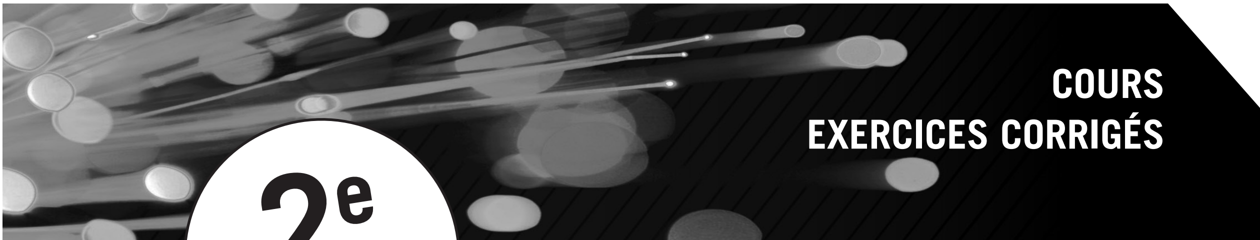
RODOT O., Analyse MP-MP*. 2e année. Cours et exercices corrigés, 2e édition

MPSI / PCSI

1re ANNÉE

Conforme aux programmes

ANALYSE



COURS
EXERCICES CORRIGÉS

2e édition

GILLES COSTANTINI

de boeck supérieur

Pour toute information sur notre fonds et les nouveautés dans votre domaine de spécialisation, consultez notre site web : **www.deboecksuperieur.com**

2e édition

Rue du Bosquet, 7 B-1348 Louvain-la-Neuve

Imprimé en Belgique

Dépôt légal :
Bibliothèque nationale, Paris : juillet 2016
Bibliothèque royale de Belgique, Bruxelles : 2016/13647/127 ISBN : 978-2-8073-0639-4

∗ Remerciements ∗

Ces quelques lignes pour adresser mes chaleureux remerciements aux différents membres de ma famille qui m'ont toujours patiemment soutenu ; à mon premier professeur de Mathématiques, en classe de sixième, Jean-Yves Bindi qui, par ses exigences m'a très tôt initié aux rigueurs de la discipline, puis à mes professeurs de l'université de Strasbourg (Michèle Audin notamment qui m'a conduit à apprécier l'algèbre et la géométrie). Un grand merci à mes collègues relecteurs, mes nombreux amis avec un clin d'œil particulier à *Bolduc* (il se reconnaîtra) qui n'a jamais douté de moi et a toujours été présent lorsqu'il le fallait.

Dans la même veine, j'adresse mes remerciements à Olivier Rodot pour ses relectures minutieuses et nombreuses remarques qui m'ont aidées à affiner les références historiques ainsi qu'à Fabrice Chrétien des éditions De Boeck Supérieur pour son pilotage logistique, son pragmatisme et sa clairvoyance.

J'adresse également ma plus vive gratitude à mes différents coordinateurs institutionnels qui, malgré les moments où la charge de travail était intense, se sont toujours montrés compréhensifs, encourageants et reconnaissants.

Et enfin, je ne peux oublier mes élèves qui, par leur intérêt et leur étonnement manifesté à chaque fois que je leur propose une escapade dans l'univers des mathématiques (comme par exemple l'équation polynomiale de degré 45 résolue par Viète, voir page 166), continuent de me conforter dans l'idée que le métier d'enseignant est le plus beau du monde.

Gilles Costantini

Avant-propos

Pour qui ? Pour quoi ?

Ce livre, d'initiation à l'analyse mathématique, est conçu en fonction des nouveaux programmes des classes préparatoires. Il est donc avant tout destiné à ce public. Mais, de nos jours, qu'est-ce qu'un étudiant de classe préparatoire ? Quels sont ses objectifs ? Avec la multiplication des filières, le public estudiantin s'est largement diversifié. Les objectifs aussi. Chez certains, on peut noter un objectif désintéressé d'apprendre juste par plaisir et par goût afin de satisfaire une soif et une curiosité intellectuelle ; chez d'autres, un objectif plus utilitaire qui est la réussite à un concours ou à un examen. Ici, tout a été mis en œuvre pour s'ouvrir et s'adapter à cette diversité.

Ainsi, chaque notion, chaque propriété est étudiée très scrupuleusement ; de nombreux exemples, contre-exemples, schémas et remarques sont donnés. Les démonstrations, des plus simples aux plus ardues, sont toujours détaillées avec le même souci : les rendre accessibles et compréhensibles au plus grand nombre. Chaque chapitre est également accompagné de questions de cours, de QCM et d'exercices systématiquement corrigés.

Tout ceci permet notamment aux élèves fraîchement issus du lycée de consolider leurs connaissances tout en les préparant au mieux aux nouveautés, afin de gommer le fameux « gouffre » entre la terminale et le supérieur. Les étudiants plus ambitieux trouveront également leur bonheur grâce aux nombreux prolongements et compléments proposés. Les parties spécifiques à la filière **MPSI** sont clairement indiquées, les **compléments** également (théorèmes sur fonds roses). Cette polyvalence permettra également aux étudiants de seconde ou troisième année de pouvoir approfondir encore certaines notions. Cet ouvrage intéressera aussi les candidats aux divers concours comme le Capes ou l'Agrégation ainsi que les étudiants des écoles d'ingénieurs ou en IUT.

Enfin, de nombreuses notes historiques sont présentées pour étayer le propos et rompre avec une tradition un peu austère du discours purement mathématique. Les théorèmes les plus importants sont datés et sourcés (lorsque c'est possible !). Ces notes ne sauraient se substituer à un ouvrage de référence en histoire des mathématiques et là, tous les détails et compléments ne sont pas forcément donnés, le but étant juste de donner envie aux étudiants d'aller parcourir les écrits d'époque, tels ceux de Viète, de Wallis, de Lagrange, de Cauchy, de Bolzano, etc. La lecture et l'analyse de ces écrits ne pourra que parfaire leur degré de compréhension des notions mathématiques ici étudiées.

Précisons maintenant, plus en détail, les
choix pédagogiques qui sont ceux de ce livre...

Prendre appui, réinvestir, anticiper et composer pour progresser.

On imagine souvent que les ouvrages mathématiques sont élaborés sur la base de progressions linéaires dans lesquelles les notions s'empilent et s'articulent progressivement les unes après les autres, générant ainsi de nombreuses références à des passages antérieurs. Une telle construction pourrait être un objectif louable mais ce n'est pas le choix qui est fait ici car cela aurait pour conséquence l'impossibilité de donner des applications riches et intéressantes dans les premiers chapitres faute de matériel suffisant. Par exemple, les notions de dérivation et d'intégration sont étudiées dans les chapitres 5 et 7 respectivement mais il serait bien dommage de s'en priver dans des situations des chapitres précédents. C'est le cas, parmi tant d'autres, de la preuve de la divergence vers $+\infty$ de la série harmonique (voir p. 263) qui utilise commodément une comparaison à une intégrale ; pourquoi faudrait-il se priver de cet outil dès le chapitre 3 ? Le lecteur ne sera donc pas surpris de voir régulièrement des références à des notions ultérieures ; ceci a le triple avantage de pouvoir présenter à l'instant t des exemples mathématiquement pertinents plutôt que basiques par manque d'éléments abordés, investir ou réinvestir un maximum de notions et préparer le terrain pour aborder plus en profondeur les chapitres ultérieurs (phénomène d'anticipation des notions). Autre exemple : si on prend – au hasard – la fonction sinus ou encore la fonction exponentielle, on la verra apparaître à tout moment : elle sera souvent considérée comme une fonction familière et connue mais certaines de ses propriétés fondamentales (comme sa continuité ou sa dérivabilité) ne seront détaillées qu'au moment venu. On ne peut pas apprendre les mathématiques en commençant par étudier tous les fondements et juste les fondements puis en terminant par les mathématiques avancées et appliquées. Non, l'idéal est de procéder par strates successives, centrées « vers le milieu » puis affiner ses connaissances en approfondissant dans deux directions : du côté des fondements et du côté de l'élaboration. D'une part, on prend ainsi appui sur ce qui est le plus familier à l'étudiant novice et d'autre part, historiquement, c'est ainsi que les différentes théories mathématiques se sont développées.

FIGURE 1 – Une progression mathématique, par **strates**.

Table des matières

CHAPITRE 1

Basic calculus...

Le lecteur « expérimenté » pourra s'épargner la lecture de ce premier chapitre de bases[1]. Elle est cependant recommandée à l'étudiant désireux de consolider ses acquis ou d'élargir ses horizons avant de s'attaquer au programme de première année de l'enseignement supérieur. En effet, dans cette introduction seront passés en revue les éléments théoriques et pratiques indispensables aux notions abordées par la suite. Idéalement, pour un bachelier ayant encore un niveau modeste en calcul, il serait bon que ce chapitre soit lu avant la rentrée en première année.

1.1 Théorie des ensembles

1.1.1 Généralités

Les ensembles[2] d'objets mathématiques sont notés à l'aide d'accolades et désignés par des majuscules. Par exemple, l'ensemble A des nombres premiers[3] inférieurs à 10 se note :

$$A = \{2\,,3\,,5\,,7\}$$

La relation d'appartenance d'un élément à un ensemble est notée $\in$.

Par exemple : $3 \in A$, mais $4 \notin A$

1. Le lecteur pourra consulter un des derniers exercices de ce premier chapitre (par ex. 1.16, p. 139) pour savoir s'il est « expérimenté » ou non !

2. Nous considérons la notion d'ensemble comme intuitive et nous ne la définirons pas rigoureusement. Disons simplement qu'un ensemble est une collection d'objets que l'on peut énumérer un à un ou définir à l'aide d'une propriété caractéristique. Cependant, des collections d'objets qui se contiennent elles-mêmes ne sont pas considérées comme étant des ensembles. Sinon cela engendrerait des situations paradoxales embarrassantes comme, par exemple, le cas de l'ensemble des ensembles qui ne se contiennent pas eux-mêmes dont on ne pourrait dire s'il se contient lui-même ou non. Ce paradoxe révélé conjointement par Ernst Zermelo et Bertrand Russel au début du XX[e] siècle a ainsi poussé les mathématiciens à baliser ce champ de mines qu'est la théorie des ensembles.

3. Voir à la page 107 pour la définition et les propriétés de base des nombres premiers.

L'ensemble qui ne possède aucun élément s'appelle *ensemble vide*, il est noté $\varnothing$.
Un ensemble ayant un seul élément est appelé un *singleton*.
Même si nous n'en ferons pas la construction rigoureuse, on suppose connus les principaux ensembles de nombres suivants :

Ensembles de nombres usuels

$\wp$: l'ensemble des nombres premiers,

$\mathbb{N}$: l'ensemble des entiers naturels,

$\mathbb{Z}$: l'ensemble des entiers relatifs,

$\mathbb{D}$: l'ensemble des nombres décimaux,[4]

$\mathbb{Q}$: l'ensemble des nombres rationnels,[5]

$\mathbb{R}$: l'ensemble des nombres réels,

$\mathbb{C}$: l'ensemble des nombres complexes.

On notera, par exemple, $\mathbb{R}_+$ l'ensemble des réels positifs ou nuls et $\mathbb{R}^*$ ou $\mathbb{R}\backslash\{0\}$ l'ensemble des réels non nuls. La notation $\mathbb{R}_+^*$ désigne ainsi l'ensemble des réels strictement positifs, la notation $\mathbb{Q}_-^*$ désigne l'ensemble des nombres rationnels strictement négatifs, etc.
Nous noterons également :

- $[\![m\,,n]\!]$ l'ensemble des entiers compris entre les entiers m et n,
- $[\![m\,,+\infty[\![$ l'ensemble des entiers qui sont supérieurs ou égaux à l'entier m,
- $[a\,,b]$ l'ensemble des réels compris entre les réels a et b,
- $[a\,,+\infty[$ (resp. $]-\infty\,,a]$) l'ensemble des réels supérieurs (resp. inférieurs) au réel a.

On dira que deux ensembles A et B sont *égaux* lorsqu'ils ont exactement les mêmes éléments. Par exemple, les ensembles $A=\{-1\,,1\}$ et $B=\big\{x\in\mathbb{R}$ tels que $x^2=1\big\}$ sont égaux. On note alors $A=B$.
On emploie parfois une barre verticale | ou oblique / pour abréger le « tel que » [6] :

$$\big\{n\in\mathbb{N}\,|\,n^2=n\big\}=\{0\,,1\}$$

4. On rappelle que les nombres *décimaux* sont ceux qui **peuvent** s'écrire sous la forme d'un développement décimal **fini** comme $\frac{1}{4}=0{,}25$ ou $\frac{13}{8}=1{,}625$. En revanche, ce n'est pas le cas de nombres tels que $\frac{1}{3}=0{,}333\ldots$ ou $\frac{22}{7}=3{,}142857142857\ldots$ qui sont des rationnels (voir note suivante) non décimaux. Ainsi, un nombre est décimal lorsqu'on peut obtenir un entier en le multipliant par une puissance de 10 : $a\in\mathbb{D}\iff a\times10^n\in\mathbb{Z}$ où $n\in\mathbb{N}$. On notera qu'il n'y a pas unicité du développement décimal, par exemple les écritures 0,5 et 0,49999… désignent le même nombre. En effet, impossible d'intercaler un réel entre les deux !

5. Les nombres *rationnels* sont ceux qui peuvent s'écrire sous la forme de fractions d'entiers comme $\frac{4}{3}$ ou $\frac{14}{11}$. Un nombre rationnel peut avoir un développement décimal illimité mais on démontre que celui-ci est toujours périodique. Cette périodicité est d'ailleurs propre aux nombres rationnels.

6. De même que, dans la langue française, un même mot peut avoir plusieurs sens (qu'il convient de saisir selon le contexte), en mathématiques, un même symbole peut également avoir plusieurs sens, c'est la cas de cette barre verticale | également employée pour signifier qu'un entier divise un autre : par exemple $3\,|\,12$ ou encore $3\nmid 11$.

Lorsque tous les éléments d'un ensemble B sont également des éléments d'un ensemble A, on dit que B est *une partie* de A ou que B est *inclus* dans A ou encore que B est un *sous-ensemble* de A.

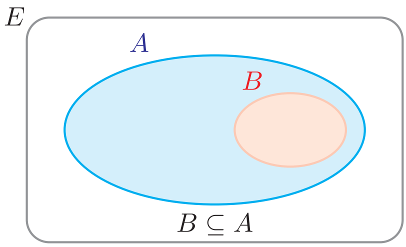


FIGURE 1.1 – Ensemble inclus dans un autre.

La relation d'inclusion[7] est notée $\subseteq$: $B \subseteq A$.
Par exemple : $\{2\,,5\} \subseteq \mathbb{N}$ ou encore $\{2\} \subseteq \mathbb{N}$

On suppose connues les inclusions strictes successives suivantes :

$$\wp \subsetneq \mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{D} \subsetneq \mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C}$$

Deux ensembles A et B sont égaux si et seulement si A est inclus dans B et B est inclus dans A :

$$A = B \iff \big(A \subseteq B \text{ et } B \subseteq A\big)$$

Ainsi, démontrer que deux ensembles sont égaux revient à démontrer les deux inclusions ci-dessus (voir l'exemple page 15).
L'ensemble des parties d'un ensemble E est noté $\mathcal{P}(E)$.
Par exemple, avec $E = \{a\,,b\,,c\}$, on a :

$$\mathcal{P}(E) = \big\{\varnothing\,,\{a\}\,,\{b\}\,,\{c\}\,,\{a\,,b\}\,,\{a\,,c\}\,,\{b\,,c\}\,,E\big\}$$

Ainsi, on a : $A \subseteq E \iff A \in \mathcal{P}(E)$

On appelle *cardinal*[8] d'un ensemble fini E son nombre d'éléments. On le note $\mathrm{Card}(E)$.
Par exemple : $\mathrm{Card}\big\{x \in \mathbb{C} \,|\, x^4 = 1\big\} = \mathrm{Card}\{-\mathbf{i}\,,\mathbf{i}\,,-1\,,1\} = 4$

Nous verrons ultérieurement diverses méthodes pour calculer le cardinal de l'ensemble des parties $\mathcal{P}(E)$ d'un ensemble fini E (voir théorème page 59).

7. L'inclusion est encore souvent notée simplement $\subset$ dans beaucoup d'ouvrages. On privilégie ici la notation $\subseteq$ (« inclus ou égal ») par analogie avec la relation d'ordre $\leqslant$. En cas d'inclusion stricte, on emploiera le symbole $\subsetneq$. Notons que de la même manière qu'il n'est pas faux d'écrire $2 \leqslant 3$, on peut légitimement écrire $\{a\} \subseteq \{a\,,b\}$, en effet si une inclusion est stricte, elle est *a fortiori* large également.
8. Nous verrons dans la section 1.9 une définition plus rigoureuse de la notion de cardinal.

1.1.2 Opérations sur les ensembles

Définissons maintenant les principaux opérateurs qui permettent, à partir d'ensembles donnés, d'en construire de nouveaux.

Définition 1

Soient A et B deux sous-ensembles d'un ensemble E.

- L'*intersection* de A et B, notée $A \cap B$, est l'ensemble des éléments de E qui appartiennent à A **et** à B :
$$x \in A \cap B \iff x \in A \textbf{ et } x \in B$$
Lorsque $A \cap B = \varnothing$, on dit que les ensembles A et B sont *disjoints*.
- L'*union* de A et B, notée $A \cup B$, est l'ensemble des éléments de E appartenant à A **ou** à B :
$$x \in A \cup B \iff x \in A \textbf{ ou } x \in B$$
Lorsque A et B sont disjoints, leur union est notée $A \amalg B$.
- Le *complémentaire* de A (dans E), noté $E \setminus A$, est l'ensemble des éléments de E n'appartenant pas à A :
$$x \in E \setminus A \iff x \in E \textbf{ et } x \notin A$$
- La *différence* de A par B, notée $A \setminus B$, est l'ensemble des éléments de A n'appartenant pas à B :
$$x \in A \setminus B \iff x \in A \textbf{ et } x \notin B$$
- La *différence symétrique* de A et B, notée $A \bigtriangleup B$, est la différence entre l'union et l'intersection, c'est-à-dire $A \bigtriangleup B = (A \cup B) \setminus (A \cap B)$:
$$x \in A \bigtriangleup B \iff x \in A \cup B \textbf{ et } x \notin A \cap B$$

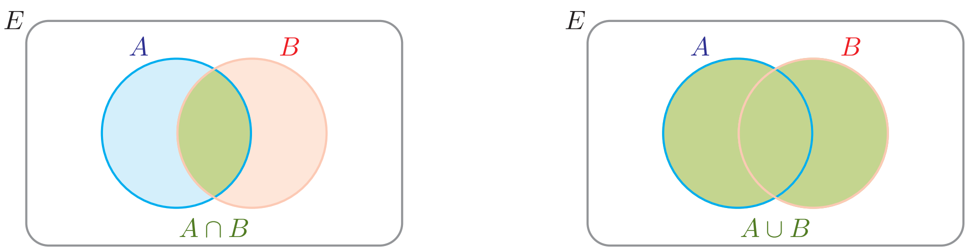


FIGURE 1.2 – Intersection et union de deux ensembles.

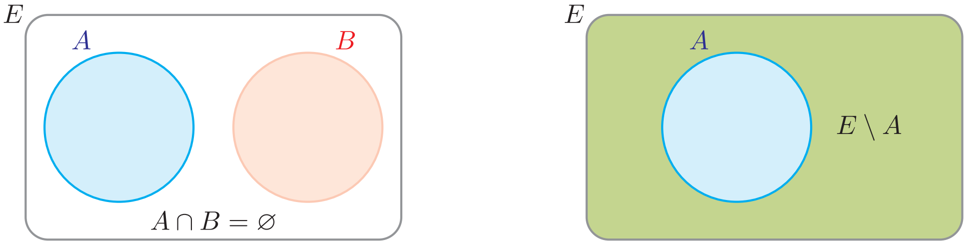


FIGURE 1.3 – Ensembles disjoints et complémentaire.

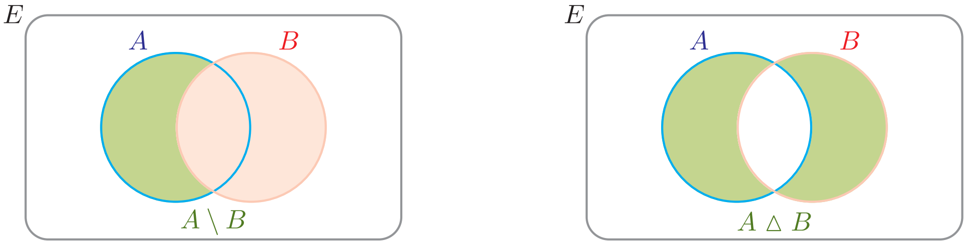


FIGURE 1.4 – Différence et différence symétrique.

Remarque

On a toujours : $A \cap B \subseteq A \subseteq A \cup B$ et $A \cap B \subseteq B \subseteq A \cup B$

Et dans le cas particulier d'une inclusion, on a :

$$B \subseteq A \iff A \cap B = B \iff A \cup B = A$$

Exemple

Démontrer que, quels que soient les ensembles A et B, on a :

$$A = (A \setminus B) \amalg (A \cap B)$$

Déjà, l'union est bien disjointe car si un élément x est dans $A \cap B$ (et donc dans B), il ne peut pas être dans $A \setminus B$.

- Soit $x \in A$.

  Si $x \in B$ alors $x \in A \cap B$.

  Si $x \notin B$ alors $x \in A \setminus B$.

  Donc on a bien : $x \in (A \setminus B) \amalg (A \cap B)$

  Ceci prouve : $A \subseteq (A \setminus B) \amalg (A \cap B)$

- Soit $x \in (A \setminus B) \amalg (A \cap B)$.

  Alors on a : $(x \in A \setminus B)$ ou $\big(x \in (A \cap B)\big)$

  Mais dans les deux cas : $x \in A$

  Ceci prouve : $(A \setminus B) \amalg (A \cap B) \subseteq A$

On a bien démontré l'égalité souhaitée.

Définition 2 (Produit cartésien)
Soient E et F deux ensembles.
On appelle *produit cartésien* de E et F, l'ensemble des couples[9] $(x\,,y)$ où $x \in E$ et $y \in F$. On note cet ensemble $E \times F$.

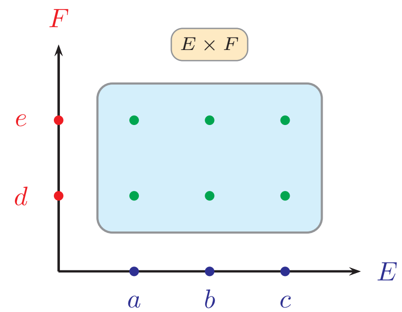
On peut faire le produit cartésien d'un ensemble E avec lui-même pour obtenir $E \times E$ que l'on notera E^2, c'est ainsi qu'on l'on construit le plan usuel $\mathbb{R}^2$.
La notion de produit cartésien peut se généraliser à n ensembles ($n \in [\![2\,,+\infty[\![$).

Exemple
Avec $E = \{a\,,b\,,c\}$ et $F = \{d\,,e\}$, on a :

$$E \times F = \big\{(a\,,d)\,,(a\,,e)\,,(b\,,d)\,,(b\,,e)\,,(c\,,d)\,,(c\,,e)\big\}$$

Illustration

Ci-contre, sont représentés :
en bleu, les éléments de E,
en rouge, les éléments de F,
et en vert, les éléments de $E \times F$.



1.2 Rudiments de logique

Nous avons utilisé dans la section précédente, à plusieurs reprises, le symbole d'équivalence $\Longleftrightarrow$ pour relier des assertions entre elles. Nous allons, dans cette section, étudier plus rigoureusement ces symboles logiques reliant les assertions. Et d'abord, qu'est-ce qu'une assertion ?
En mathématiques, vous l'avez sûrement remarqué, il existe des affirmations qui sont vraies et d'autres fausses[10]. Mais cette nature binaire ne s'applique pas à toutes les affir-

9. La notion de couple est difficile à définir. Une façon de procéder est de travailler sur $\mathcal{P}(E \cup F)$ et de définir un couple $(x\,,y)$ par identification à la partie $\big\{\{x\}\,,\{x\,,y\}\big\}$ de $\mathcal{P}(E \cup F)$. Ainsi, $(x\,,y)$ et $(y\,,x)$ sont des couples différents en général.

10. Il en existe également des *indécidables* telle la déclaration d'Épiménide le crétois qui déclarait : « tous les crétois sont des menteurs ». Ce paradoxe du menteur peut se synthétiser de manière logique de la façon suivante :

Théorème 1 - Le théorème 1 est faux.

Un tel théorème, s'il est vrai est alors faux et s'il est faux, est vrai ! On peut penser qu'une façon d'éviter ce genre de paradoxe est de bannir les auto-références. Malheureusement, cela ne se révélera pas suffisant et le logicien Kurt Gödel démontrera en 1931 que l'indécidabilité existe au sein même de l'arithmétique...

mations. Si j'affirme « je pense qu'il va pleuvoir demain » ou encore « cette suite semble croissante » ou encore « on obtient le chiffre 3 en lançant un dé » ou encore « $x^2 - 4 = 0$ », il n'est pas possible de donner un statut tranché (vrai ou faux) à de telles affirmations. Soit parce que l'affirmation contient un caractère aléatoire, soit parce qu'elle contient un élément relatif à l'émotionnel, soit parce que son champ d'application est insuffisamment précisé. Nous allons nous intéresser, ici, seulement aux affirmations ou phrases pour lesquelles se pose la question de sa vérité ou non. De telles phrases s'appellent des *assertions*. Par exemple, la phrase p ci-dessous :

$$p : \text{ « } 27 \times 40 = 1080 \text{ »}$$

est bien une assertion (qui, en l'occurrence, est vraie).
De même, la phrase q suivante :

$$q : \text{ « } (1828 - 1797)^2 = 956 \text{ »}$$

est également une assertion (bien sûr fausse).
En revanche, comme on l'a précisé ci-dessus, des phrases telles que « bienvenue ! » ou encore « du plus profond du cœur ! » ne sont pas des assertions car cela n'a aucun sens de se poser la question de savoir si elles sont vraies ou fausses. Il y a également des phrases qui ne sont pas des assertions car mal formulées comme « $1791 - 1756 =$ ».
Selon le contexte, une même assertion peut avoir un statut différent comme par exemple « il fait jour » qui est vraie ou fausse selon l'heure qu'il est ou l'endroit où l'on se situe. De même, l'assertion « l'équation $x^2 = 9$ possède une seule solution » est vraie dans l'ensemble $\mathbb{N}$ des entiers naturels et fausse dans l'ensemble $\mathbb{Z}$ des entiers relatifs. Autre exemple : l'assertion « 2 divise n » n'a un sens que si n est entier et n'est vraie que si n est pair. Enfin, certaines assertions contiennent également des éléments variables qui les rendent vraies ou fausses selon la valeur de ces variables. Par exemple, l'assertion « x est une solution réelle de l'équation $x^3 = -1$ » est vraie si $x = -1$ mais fausse si $x = 0$.

Exemple

Considérons l'assertion suivante :

$$\text{« l'inéquation } \frac{x-9}{2-x} \geqslant 0 \text{ possède exactement sept solutions »}$$

Déterminer un ensemble de nombres pour lesquels cette affirmation est vraie et un ensemble de nombres pour lesquels elle est fausse[11].

Nous disposons de *connecteurs logiques* pour fabriquer des assertions plus élaborées à partir d'assertions élémentaires. Ces connecteurs sont la conjonction (« et »), la disjonc-

11. Si on considère l'inéquation à résoudre sur l'ensemble $\mathbb{Z}$, l'affirmation est vraie mais elle fausse si l'ensemble de résolution est $\mathbb{R}$

tion (« ou »), la négation (« non ») et bien d'autres encore.

Par exemple, pour x réel et avec les assertions p : « $x \geqslant 3$ » et q : « $0 \leqslant x < 5$ », on peut former les assertions suivantes :

- p et q : « $x \geqslant 3$ et $0 \leqslant x < 5$ », c'est-à-dire $3 \leqslant x < 5$;
- p ou q : « $x \geqslant 3$ ou $0 \leqslant x < 5$ », c'est-à-dire $x \in \mathbb{R}_+$;
- non(p)[12] : « $x < 3$ ».

Le caractère de vérité de ces assertions combinées dépend de celui de p et de q. On peut dresser la liste des états (vrai ou faux)[13] d'une assertion combinée en fonction des états de son ou ses arguments. Une telle liste s'appelle une *table de vérité*.

On peut ainsi définir précisément la conjonction (ET) de deux assertions (p et q) qui est vraie uniquement lorsque les assertions p et q sont toutes les deux vraies.

On définit également da disjonction (OU)[14] de deux assertions (p ou q) qui est vraie lorsque l'une ou l'autre est vraie (les deux pouvant l'être en même temps).

Conjonction **ET**		
p	q	p et q
0	0	0
0	1	0
1	1	1
1	0	0

Disjonction **OU**		
p	q	p ou q
0	0	0
0	1	1
1	1	1
1	0	1

Négation **NON**	
p	non(p)
0	1
1	0

FIGURE 1.5 – Table de vérité des connecteurs logiques de base.

On peut former, en tout, $2^4 = 16$ connecteurs logiques à partir de deux assertions p et q comme arguments. On peut démontrer que l'on peut engendrer ces 16 connecteurs à partir de la conjonction et la négation. Par exemple, la disjonction (p ou q) possède toujours les mêmes valeurs de vérité que l'assertion $\text{non}\big(\text{non}(p)$ et $\text{non}(q)\big)$ comme le montre la table de vérité ci-dessous :

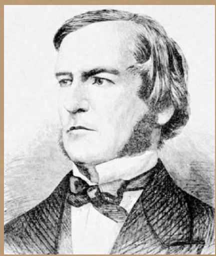
p	q	non(p)	non(q)	non(p) et non(q)	$\text{non}\big(\text{non}(p)$ et $\text{non}(q)\big)$
0	0	1	1	1	0
0	1	1	0	0	1
1	1	0	0	0	1
1	0	0	1	0	1

FIGURE 1.6 – Une assertion logique ayant même valeur de vérité que (p ou q).

12. Les logiciens notent souvent la négation avec le symbole $\neg$. Par exemple, en logique classique $\neg\neg p$ (double négation) équivaut à p. Dans un contexte ensembliste, la négation se note parfois autrement. En effet, ne pas appartenir à un ensemble A, c'est appartenir à son complémentaire noté C_A ou encore $\overline{A}$. On retrouve cette notation dans le langage des événements en théorie des probabilités.

13. Les logiciens adoptent la convention 0 pour coder le faux et le 1 pour coder le vrai.

14. Ce connecteur « OU » des logiciens (dit « OU inclusif ») est à distinguer de « OU exclusif » que nous utilisons dans notre langage courant. Si l'on vous propose une sortie au cinéma ou à l'opéra, c'est rarement les deux à la fois ! Ce « OU exclusif » du langage courant (l'un ou l'autre mais pas les deux simultanément) est représenté par les logiciens par la *différence symétrique* notée Δ.



George Boole
(1815–1864)

Né à Lincoln en Angleterre, issu d'une famille modeste, George Boole est contraint de s'instruire en autodidacte. Il apprend notamment les langues puis les enseigne pour aider son père, cordonnier, dont les affaires ne sont guère florissantes. N'allant ainsi pas à l'école, George Boole n'obtient pas de diplôme universitaire ce qui ne l'empêche pas de créer son propre institut d'enseignement dans sa ville natale dès l'âge de 19 ans. En 1838, il succède à Robert Hall à la tête de la « Hall-Academy » de Waddington et commence à rédiger des publications régulières en algèbre et en analyse suite à l'étude des œuvres de Laplace[a] et Lagrange[b]. Dans les années 1840, il travaille étroitement avec De Morgan[c] à la résolution algébrique d'équations différentielles. Grâce à ces travaux, sa renommée grandissante lui permet d'obtenir une chaire au collège de Cork en 1849. C'est là qu'il rencontre la jeune mathématicienne Mary Everest[d]. Ils fondent une famille unie : les cinq filles issues de cette union se consacrent aux mathématiques également ! C'est dans son ouvrage *Mathematical Analysis of Logic*[e] que George Boole modélise les lois de la logique sous forme d'une algèbre (dite de Boole) très utilisée encore de nos jours dans les ordinateurs et les réseaux téléphoniques.
On retiendra de George Boole de nombreux articles sur les équations différentielles[f], le calcul des différences finies[g], les probabilités et sa démarche générale pour rattacher la logique aux mathématiques.
George Boole meurt en 1864 d'une pneumonie après avoir marché deux miles sous la pluie et dispensé une conférence transi de froid dans ses vêtements trempés.

a. cf. notice biographique page 770.
b. cf. notice biographique page 489.
c. cf. notice biographique page 21.
d. nièce de George Everest, célèbre géographe connu pour avoir, en 1852, dirigé les opérations de cartographie de la plus haute montagne du monde qui porte désormais son nom.
e. Précisément *The Mathematical Analysis of Logic, Being an Essay towards a Calculus of Deductive Reasoning*, Barclay et MacMillan, Londres (1847).
f. cf. *A treatise on differential equations*, MacMillan, Londres (1860).
g. cf. *A treatise on the calculus of finite differences*, MacMillan, Londres (1859).

Remarque historique

Plus généralement, le mathématicien George Boole étudia les propriétés de ces connecteurs logiques et observa une certaine analogie[15] avec les opérations usuelles comme $\times$ et $+$. Il put, ainsi, définir une algèbre faite de règles (élément neutre, distributivité, simplification) permettant de réduire des fonctions logiques complexes.
Ainsi, on peut définir des règles sur les combinaisons d'assertions logiques elles-mêmes, combinaisons que nous appellerons *expressions booléennes*.

15. Cette analogie a des limites et nous ne l'emploierons pas ici par risque de confusion. En effet, en algèbre de Boole on a par exemple : $p + p = p$ (p ou p, c'est p), $p + 1 = p$ (p ou du vrai, c'est encore p !)

Définition 3

Lorsque deux expressions booléennes $A(p,q)$ et $B(p,q)$ qui dépendent des mêmes arguments p et q ont les mêmes valeurs de vérité, on dit qu'elles sont *logiquement équivalentes* et on note :

$$A(p,q) \equiv B(p,q)$$

Ce symbole $\equiv$ est un « métasymbole » puisqu'il ne porte plus sur des propriétés mathématiques elles-mêmes mais sur les liens logiques qui unissent les formulations de ces propriétés mathématiques d'où la nécessité d'utiliser un symbole spécifique (et pas $\Longleftrightarrow$) pour ne pas tout mélanger. Ainsi, la table de vérité ci-dessus montre que :

$$(p \text{ ou } q) \ \equiv \ \text{non}\big(\text{non}(p) \text{ et } \text{non}(q)\big)$$

Théorème 1 (Lois de De Morgan (1839)[16])

Soient A et B des expressions booléennes. En notant $\overline{A}$ la négation de A, on a :

$$\overline{A \text{ et } B} \equiv \overline{A} \text{ ou } \overline{B} \quad \text{ et } \quad \overline{A \text{ ou } B} \equiv \overline{A} \text{ et } \overline{B}$$

Démonstration

Il suffit d'écrire les tables de vérité des expressions en question comme ci-avant.

Remarque

On notera l'analogie entre les lois de De Morgan et les relations ensemblistes suivantes lorsque A et B sont deux parties d'un ensemble E :

$$E \setminus (A \cap B) = (E \setminus A) \cup (E \setminus B) \ \text{ et } \ E \setminus (A \cup B) = (E \setminus A) \cap (E \setminus B)$$

Ces relations sont démontrées dans l'exercice 1.1, page 122.

Précisons également les tables de vérité de **l'implication** $(p \Longrightarrow q)$ ainsi que de **l'équivalence** mathématique $(p \Longleftrightarrow q)$.

- L'implication $p \Longrightarrow q$ est définie par l'expression booléenne : q ou non(p). Autrement dit, une implication $p \Longrightarrow q$ est vraie lorsque q est vraie ou lorsque p est fausse. En utilisant les lois de De Morgan, on a également :

$$q \text{ ou } \overline{p} \ \equiv \ \overline{\overline{q} \text{ et } p}$$

  Autrement dit, l'implication $p \Longrightarrow q$ est ainsi vraie sauf quand l'assertion p est vraie et l'assertion q fausse.

  Comme on pourra le constater sur la table de vérité ci-dessous, le faux peut donc entraîner autant le vrai comme le faux, ainsi l'assertion « si $1 = 2$ alors $3 = 3$ » est, du

16. cf. *First notions of logic, Preparatory to the study of Geometry*, **1**, Taylor and Walton, Londres.

Auguste De Morgan
(1806–1871)

Fils d'un colonel de l'armée des Indes, Auguste De Morgan naît à Madurai dans le sud de l'Inde. Mais à cause de révoltes locales, le père renvoie sa famille en Angleterre. Ayant perdu la vue à l'œil droit peu après sa naissance, le petit Auguste De Morgan est sujet aux brimades et moqueries de ses camarades. Il n'est d'ailleurs pas un brillant élève et déteste les examens. Mais, tirant force de son handicap, il réalise de brillantes études de droit à Londres et obtient un poste de professeur de mathématiques à l'université en 1827 ; il n'est alors âgé que de 21 ans !
Il s'intéresse à l'arithmétique[a], à la logique[b,c] ainsi qu'à la trigonométrie[d].
En 1866, il fonde la Société mathématique de Londres (qu'il préside) et est élu à la Société royale d'astronomie.
De Morgan s'intéresse également à l'histoire des mathématiques, à la philosophie et à la musique, c'est un excellent flûtiste. Sa bibliothèque personnelle contient plus de 3000 livres !

a. cf. *Elements of arithmetic*, Taylor and Walton, Londres (1830).
b. cf. sa contribution à l'encyclopédie *The Penny Cyclopaedia* de la Society for the Diffusion of Useful Knowledge pour ses explications et exemples sur l'induction mathématique.
c. cf. *First notions of logic, Preparatory to the study of Geometry*, Taylor and Walton, Londres (1839), contenant les lois de De Morgan et son œuvre maîtresse *Formal logic of the Calculus of Inference*, Taylor and Walton, Londres (1847).
d. cf. *Trigonometry and double algebra*, Walton and Malbery, Londres (1849) où l'on y trouve une interprétation géométrique des nombres complexes qu'il décrit comme un ensemble bénéficiant d'une « algèbre double » ; il tente, de plus, d'étendre ces propriétés pour construire une algèbre triple décrivant notre espace mais se heurte à de nombreuses difficultés dans cette construction.

point de vue de la logique, une affirmation vraie (très facile à prouver d'ailleurs car si $1 = 2$ alors $2 = 1$ et ajoutant membre à membre les deux égalités, on obtient $3 = 3$). Cependant, le vrai n'implique jamais le faux !

Vocabulaire lié à l'implication $p \Longrightarrow q$

Pour avoir q, *il suffit* d'avoir p

Pour que p se réalise, *il faut* que q se réalise

p est une condition *suffisante* pour q

q est une condition *nécessaire* pour p

- L'équivalence $p \Longleftrightarrow q$ est définie par ($p \Longrightarrow q$ et $q \Longrightarrow p$). Ainsi, une équivalence est vraie lorsque les deux assertions p et q auront la même valeur de vérité (toutes les deux vraies ou[17] toutes les deux fausses).

17. Ce « ou » est exclusif ! C'est le « ou » du langage courant.

Implication $\Longrightarrow$		
p	q	$p \Longrightarrow q$
0	0	1
0	1	1
1	1	1
1	0	0

Équivalence $\Longleftrightarrow$		
p	q	$p \Longleftrightarrow q$
0	0	1
0	1	0
1	1	1
1	0	0

FIGURE 1.7 – Table de vérité de l'implication et de l'équivalence.

Insistons sur le fait qu'il est utile de connaître la négation d'une implication :

$$\text{non}(p \Longrightarrow q) \;\equiv\; p \text{ et non}(q)$$

En effet, par définition $p \Longrightarrow q$ c'est $\big(q \text{ ou non}(p)\big)$ donc par négation, cela donne $\text{non}\big(q$ ou $\text{non}(p)\big)$ et d'après les lois de De Morgan, on obtient bien $(\text{non}(q)$ ou $p)$.
On ne confondra pas la négation avec la *contraposée* d'une implication qui est définie par $\text{non}(q) \Longrightarrow \text{non}(p)$ et qui est une assertion logiquement équivalente à l'implication directe $p \Longrightarrow q$. En voici, une preuve en terme de logique :

$$\big(\text{non}(q) \Longrightarrow \text{non}(p)\big) \;\equiv\; \Big(\text{non}\big(\text{non}(q)\big) \text{ ou non}(p)\Big) \;\equiv\; \big(q \text{ ou non}(p)\big) \;\equiv\; (p \Longrightarrow q)$$

Ce que l'on peut également vérifier à l'aide d'une table de vérité.

Exemple

Démontrons que l'assertion $\big(p \text{ et } (p \Longrightarrow q)\big) \Longrightarrow q$ est toujours vraie[18] :

p	q	$p \Longrightarrow q$	p et $(p \Longrightarrow q)$	$\big(p \text{ et } (p \Longrightarrow q)\big) \Longrightarrow q$
0	0	1	0	1
0	1	1	0	1
1	1	1	1	1
1	0	0	0	1

FIGURE 1.8 – Règle de détachement (ou *modus ponens*).

Textuellement : si on a p d'une part, et si, d'autre part, on sait que p implique q, alors on est assuré d'avoir q.

18. Une assertion toujours vraie s'appelle une *tautologie*. Dans le cas présent, on peut noter : $\big(p \text{ et } (p \Longrightarrow q)\big) \Longrightarrow q \equiv 1$.

1.3 Fonctions et applications

Définition 4 (Relation)

Soient E et F deux ensembles.

On appelle *relation* $\mathcal{R}$ tout triplet $(E\,,F\,,\Gamma)$ où Γ est une partie de $E \times F$.

On dit que E est l'ensemble de départ de $\mathcal{R}$ et F l'ensemble d'arrivée de $\mathcal{R}$.

L'ensemble Γ s'appelle le *graphe* de la relation $\mathcal{R}$.

Soient $x \in E$ et $y \in F$. Lorsque $(x\,,y) \in \Gamma$, on dit que x est en relation avec y et on note $x\mathcal{R}y$. L'élément y est alors appelé *une image* de x tandis que l'élément x est appelé *un antécédent* de y.

Lorsque $E = F$, on parle alors de relation *binaire* et on verra à la page 153 une autre façon de la définir.

Exemple

Notons $E = F = \mathbb{R}$. L'ensemble des couples $(x\,,y)$ de $\mathbb{R}^2$ qui vérifient $y^2 = x$ définit une relation $\mathcal{R}$ dont le graphe Γ est représenté ci-dessous.

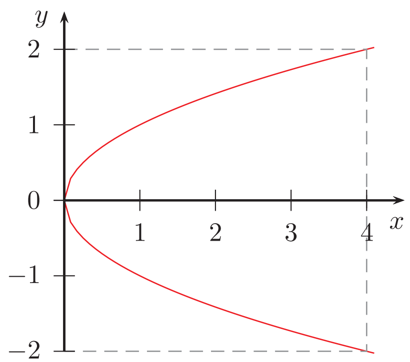


FIGURE 1.9 – Le graphe, dans $\mathbb{R}^2$, de la relation $y^2 = x$.

Notons que, par cette relation, le nombre $x = 4$ possède deux images qui sont 2 et -2.

On note : $$4\mathcal{R}2 \text{ et } 4\mathcal{R}(-2)$$

Notons également que, en général, une relation n'est pas symétrique. Sur l'exemple ci-dessus, on a $4\mathcal{R}2$ mais on n'a pas $2\mathcal{R}4$.

Définition 5 (Fonction)

Soient E et F deux ensembles.

On appelle *fonction* f de E dans F toute relation $\mathcal{R}$ dans laquelle chaque élément x de E est en relation avec **au plus un** élément y de F. Cet élément y, lorsqu'il existe, est appelé *l'image* de x par f et on note $y = f(x)$.

On appelle *ensemble (ou domaine) de définition* de la fonction f l'ensemble des éléments de E pour lesquels une image existe.

Exemple

Notons $E = F = \mathbb{R}$. L'ensemble des couples (x, y) de $\mathbb{R}^2$ qui vérifient $y = \sqrt{x}$ définit une fonction f dont le graphe Γ est représenté ci-dessous. En effet, chaque réel admet au plus une racine carrée. L'ensemble de définition de cette fonction est $\mathbb{R}_+$.

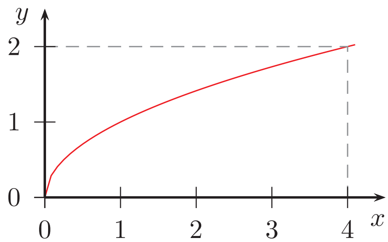


FIGURE 1.10 – Le graphe, dans $\mathbb{R}^2$, de la fonction définie par $y = \sqrt{x}$.

Définition 6 (Application)

Soient E et F deux ensembles.

On appelle *application* f de E dans F toute fonction pour laquelle chaque élément x de E admet **exactement une** image y dans F.

L'ensemble des applications de E dans F est noté $\mathrm{App}(E, F)$ ou encore F^E.

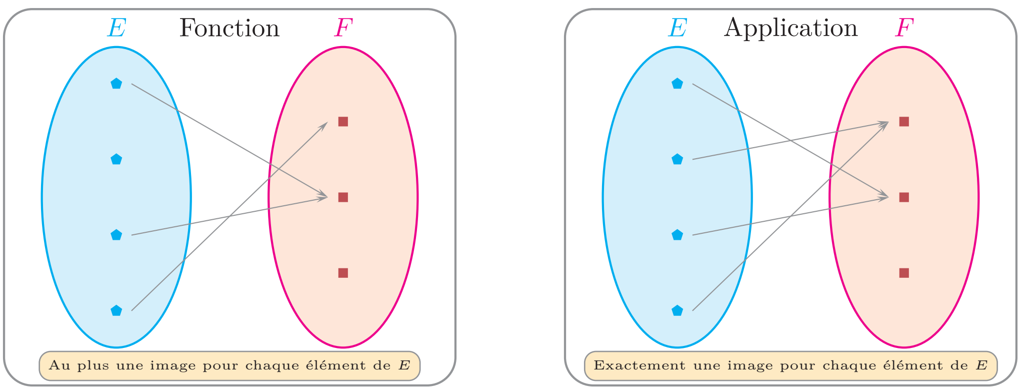


FIGURE 1.11 – Fonction et application.

Exemple

$E = \mathbb{R}_+$, $F = \mathbb{R}$ et f définie par $f(x) = \sqrt{x}$.

Remarque

Une fonction restreinte à son ensemble de définition est donc une application.

Notation

Une application f d'un ensemble E dans un ensemble F sera souvent notée selon le schéma fonctionnel suivant :

$$\begin{array}{rccc} f: & E & \longrightarrow & F \\ & x & \longmapsto & f(x) \end{array}$$

Convention importante

On se permettra également d'utiliser le schéma ci-dessus pour les fonctions mais, dans ce cas, l'ensemble de départ sera inclus dans l'ensemble de définition de la fonction. Ainsi, pour la fonction logarithme népérien, on notera :

$$\begin{array}{rccc} f: & \mathbb{R}_+^* & \longrightarrow & F \\ & x & \longmapsto & \ln(x) \end{array}$$

Ainsi, dans cet ouvrage, le fait d'évoquer une fonction sous la forme $f : E \longrightarrow F$ sous-entend que la fonction en question est **bien définie** sur E.

Définition 7 (Image directe, image réciproque)

Soit $f : E \longrightarrow F$ une application (ou une fonction).

On appelle *image directe* d'une partie A de E l'ensemble $f(A) = \{f(x), x \in A\}$.

En particulier, l'ensemble $f(E)$ s'appelle *l'image* de f encore notée $\mathrm{Im}(f)$.

On appelle *image réciproque* d'une partie B de F l'ensemble :

$$f^{-1}(B) = \{x \in E \mid f(x) \in B\}$$

En particulier, pour $y \in F$, l'ensemble $f^{-1}(\{y\})$ s'appelle la *fibre* de y par f.

On peut dire que $f(A)$ est l'ensemble des images des éléments de A et $f^{-1}(B)$ est l'ensemble des antécédents éventuels des éléments de B.

Remarque

On peut considérer f^{-1} comme une application de $\mathcal{P}(F)$ dans $\mathcal{P}(E)$.[19]

19. On ne confondra pas l'application « fibre » f^{-1} (parfois notée encore $\overset{-1}{f}$) avec l'éventuelle bijection réciproque, notée également f^{-1} (voir la définition 11, page 46). La bijection réciproque f^{-1} d'une bijection f est, en effet, une application de F dans E. Ceci dit, lorsque f est bijective, on a alors :

$$\forall y \in F,\ \overset{-1}{f}\big(\{y\}\big) = \big\{f^{-1}(y)\big\}$$

Autrement dit, la fibre du singleton $\{y\}$ est le singleton contenant l'antécédent de y.

Exemples

- Avec la fonction f définie pour tout $x \in \mathbb{R}$ par $f(x) = \sin(x)$, on a :
$$f\left(\left[0\,,\frac{\pi}{6}\right]\right) = \left[0\,,\frac{1}{2}\right] \text{ et } f^{-1}\big(\{0\}\big) = \{k\pi,\ k \in \mathbb{Z}\}$$
La fibre de 0 par la fonction sinus est donc l'ensemble des multiples de π.
- Avec la fonction f définie pour tout $x \in \mathbb{R}$ par $f(x) = x^2$, on a :
$$f\big([1\,,2[\big) = [1\,,4[\text{ et } f^{-1}\big([1\,,4[\big) =]-2\,,1] \cup [1\,,2[$$

On peut constater que, dans ce dernier exemple, on a l'inclusion stricte :
$$[1\,,2[\subsetneq f^{-1}\Big(f\big([1\,,2[\big)\Big)$$
Ainsi, une partie A de E et la partie « aller – retour » $f^{-1}\big(f(A)\big)$ ne coïncident pas nécessairement. On a cependant toujours une inclusion dans un sens comme le montre le théorème suivant.

Théorème 2

Soit $f : E \longrightarrow F$ une application (ou une fonction).

Soient $A \in \mathcal{P}(E)$ et $B \in \mathcal{P}(F)$. Alors :
$$A \subseteq f^{-1}\big(f(A)\big) \text{ et } f\big(f^{-1}(B)\big) \subseteq B$$

Démonstration

Montrons $A \subseteq f^{-1}\big(f(A)\big)$.
Soit $a \in A$. Posons $b = f(a)$, donc par définition $b \in f(A)$.
Comme a est un antécédent de b, il fait partie de l'ensemble des antécédents de $f(A)$.
Donc $a \in f^{-1}\big(f(A)\big)$ d'où l'inclusion souhaitée.
Montrons $f\big(f^{-1}(B)\big) \subseteq B$.
Soit $b \in f\big(f^{-1}(B)\big)$. Cela signifie qu'il existe $a \in f^{-1}(B)$ tel que $f(a) = b$.
Mais dire que $a \in f^{-1}(B)$ signifie qu'il existe b' dans B tel que $f(a) = b'$.
Donc $b = b'$ et par suite $b \in B$ d'où l'inclusion voulue.

Remarque

Les inclusions de ce théorème sont « larges », cela signifie qu'il peut donc y avoir, selon les caractéristiques[20] de f, égalité entre les parties A et $f^{-1}\big(f(A)\big)$ de même qu'il peut y avoir égalité entre les parties B de $f\big(f^{-1}(B)\big)$. Mais ces égalités ne sont pas des généralités, on a déjà vu un contre-exemple précédemment où l'on avait $A \subsetneq f^{-1}\big(f(A)\big)$. De même pour l'autre inclusion, si on considère maintenant que f est la fonction exponentielle, on a par exemple $f\big(f^{-1}(\mathbb{R})\big) = f(\mathbb{R}) = \mathbb{R}_+^*$ donc dans ce cas $f\big(f^{-1}(B)\big) \subsetneq B$.

Théorème 3 (Images réciproques et complémentaire)

Soit $f : E \longrightarrow F$ une application (ou une fonction).

Soit $B \in \mathcal{P}(F)$. Alors :

$$f^{-1}(F \setminus B) = E \setminus f^{-1}(B)$$

Autrement dit, l'image réciproque d'un complémentaire est égale au complémentaire de l'image réciproque.

Démonstration

Procédons par double inclusion.
Si $f^{-1}(F \setminus B) = \varnothing$, on a nécessairement l'inclusion $f^{-1}(F \setminus B) \subseteq E \setminus f^{-1}(B)$.
Supposons $f^{-1}(F \setminus B) \neq \varnothing$ et soit $x \in f^{-1}(F \setminus B)$.
Il existe donc $y \in F \setminus B$ tel que $y = f(x)$.
Mais puisque $y \notin B$, on a $f(x) \notin B$, autrement dit l'image de x n'est pas dans B.
Ainsi, l'ensemble des antécédents des éléments de B ne contient pas x :

$$x \notin f^{-1}(B)$$

Ce qui signifie : $$x \in E \setminus f^{-1}(B)$$

D'où l'inclusion : $$f^{-1}(F \setminus B) \subseteq E \setminus f^{-1}(B)$$

Réciproquement si $E \setminus f^{-1}(B) = \varnothing$, on a alors l'inclusion $E \setminus f^{-1}(B) \subseteq f^{-1}(F \setminus B)$.
Supposons $E \setminus f^{-1}(B) \neq \varnothing$ et soit $x \in E \setminus f^{-1}(B)$.
Donc $x \notin f^{-1}(B)$, autrement dit aucun élément de B n'a x pour antécédent.
Donc : $$f(x) \notin B$$

En effet, si on avait $f(x) \in B$, alors on aurait $x \in f^{-1}(B)$ ce qui n'est pas le cas.
On a donc : $$f(x) \in F \setminus B$$

D'où : $$x \in f^{-1}(F \setminus B)$$

D'où l'inclusion : $$E \setminus f^{-1}(B) \subseteq f^{-1}(F \setminus B)$$

On en déduit bien l'égalité souhaitée.

20. En fait, on a toujours $A \subseteq f^{-1}\big(f(A)\big)$ avec égalité si et seulement si f est une injection et on a toujours $f\big(f^{-1}(B)\big) \subseteq B$ avec égalité si et seulement si f est une surjection (sur B). Voir à la page 43 les définitions d'injection et de surjection.

Remarque

Il n'y a pas de propriété équivalente avec les images directes. Même pas d'inclusion simple. Voici un contre-exemple : prenons une fonction $f : \mathbb{R} \longrightarrow \mathbb{R}$ constante égale à k. Considérons la partie $A = [-1\,,1]$. On a :

$$f(A) = \{k\} \text{ et } f\big(\mathbb{R} \setminus A\big) = \{k\}$$

Donc $\mathbb{R} \setminus f(A) = \mathbb{R} \setminus \{k\}$, ce qui n'est pas égal à $f\big(\mathbb{R} \setminus A\big)$.
Moralité : les images réciproques sont plus « sympathiques » que les images directes ! Cela est dû au fait qu'un élément de l'ensemble d'arrivée peut avoir plusieurs antécédents donc si $A \in \mathcal{P}(E)$, il peut arriver qu'il existe $x \in E \setminus A$ tel que $f(x) \in f(A)$.

1.4 Quantificateurs

Deux quantificateurs sont très employés en mathématiques :
- le quantificateur *universel* « *quel que soit* » noté $\forall$;
- le quantificateur *existentiel* « *il existe (au moins un)* » noté $\exists$.

Ainsi, pour exprimer le fait que l'exponentielle de tout nombre réel est strictement positive, on notera :

$$\forall x \in \mathbb{R},\ \mathbf{e}^x > 0$$

Pour exprimer le fait que tout entier naturel impair n s'écrit de la forme $n = 2k + 1$ où $k \in \mathbb{N}$ on notera :

$$n \text{ entier naturel impair } \iff (\exists k \in \mathbb{N},\ n = 2k + 1)$$

Lorsqu'il existe **un unique** objet vérifiant telle ou telle propriété, on note « $\exists!$ » :

$$\exists! x \in \mathbb{R}_+^*,\ \ln(x) = 1$$

Certaines assertions mathématiques peuvent contenir successivement plusieurs quantificateurs. Par exemple, pour exprimer qu'une fonction f définie sur $\mathbb{R}$ est majorée sur un intervalle I par un certain réel M on notera :

$$\exists M \in \mathbb{R},\ \forall x \in I,\ f(x) \leqslant M$$

Pour obtenir la négation d'une phrase quantifiée, on remplace $\forall$ par $\exists$ (et vice-versa) et l'affirmation finale par sa négation. Ainsi, on exprime qu'une fonction f définie sur $\mathbb{R}$ n'est pas majorée sur I en notant :

$$\forall M \in \mathbb{R},\ \exists x \in I,\ f(x) > M$$

(Quel que soit le réel M choisi, on peut trouver un réel x de I tel que $f(x)$ dépasse M)

L'ordre des quantificateurs est important et ne peut pas, en général, être modifié.

Par exemple, les deux assertions suivantes :

$$\forall a \in \mathbb{R}_+\,, \exists x \in \mathbb{R},\ x^2 = a$$

et :

$$\exists x \in \mathbb{R},\ \forall a \in \mathbb{R}_+\ x^2 = a$$

n'ont pas du tout la même signification. La première assertion exprime le fait que l'équation $x^2 = a$ admet au moins une solution réelle lorsque a est positif. Tandis que la seconde assertion est clairement fausse : existe-t-il un réel x dont le carré est égal à tout réel positif a ? Clairement non.

En revanche, l'ordre des quantificateurs peut être modifié lorsqu'ils sont de même nature (que des $\forall$ ou que des $\exists$) et qu'ils prélèvent des objets de façon indépendante comme dans l'assertion suivante :

$$\forall x \in \mathbb{Q}, \forall y \in \mathbb{Q},\ (x + y \in \mathbb{Q} \text{ et } x \times y \in \mathbb{Q})$$

Et dans ce cas on peut noter « $\forall x, y \in \mathbb{Q}, \dots$ » ou encore « $\forall (x\,, y) \in \mathbb{Q}^2, \dots$ ».

Le contre-exemple

Pour démontrer qu'une assertion du type :

$$\forall x \in E,\ \mathcal{P}(x)$$

est **fausse**, il suffit d'exhiber un contre-exemple :

$$\exists x \in E,\ \text{non}\big(\mathcal{P}(x)\big)$$

Illustrons : l'assertion « $\forall n \in \mathbb{N},\ n^2 + n + 41$ est un nombre premier » est-elle vraie ?

On peut vérifier que c'est le cas pour tous les entiers $n \in [\![0\,, 39]\!]$ mais pour $n = 40$, on a : $40^2 + 40 + 41 = 40(40 + 1) + 41 = 40 \times 41 + 41 = 41(40 + 1) = 41^2$ qui est un nombre composé. L'affirmation est donc fausse puisqu'on a trouvé un contre-exemple. (C'est le mathématicien Leonhard Euler (1707-1783, voir page 267) qui proposa[21], en 1772, ce polynôme $X^2 + X + 41$ qui génère beaucoup de nombres premiers lorsque $X \in \mathbb{N}$.)

1.5 Différents types de raisonnements logiques

Abordons plus en détail deux types de raisonnements classiques en mathématiques : le raisonnement par contraposition et le raisonnement par l'absurde et essayons de décortiquer leur structure logique.

21. cf. *Extrait d'une lettre de M. Euler le père à M. Bernoulli concernant le mémoire imprimé parmi ceux de 1771*, Nouveaux Mémoires de l'Académie royale des Sciences, Berlin, pp. 335-337.

Exemple 1

Soit $n \in \mathbb{Z}$. Démontrer que : $\quad n^2$ pair $\implies n$ pair

Une façon de démontrer cette implication est de dire :

Supposons n impair, alors il existe un entier $k \in \mathbb{Z}$ tel que $n = 2k+1$ et par suite :

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1$$

Comme $4k^2$ et $4k$ sont des entiers pairs, on en déduit que n^2 est impair.

On a ainsi prouvé : $\quad n$ impair $\implies n^2$ impair

D'où, par contraposition : $\quad n^2$ pair $\implies n$ pair

Exemple 2

Soit $f : I \longrightarrow \mathbb{R}$ une fonction croissante (où I est un intervalle).

Soient a et b dans I. Démontrer que :

$$f(a) < f(b) \implies a < b$$

Une façon de démontrer cette implication est de dire :

Supposons $a \geqslant b$. Alors par croissance de la fonction f sur I :

$$f(a) \geqslant f(b)$$

On a ainsi prouvé : $\quad a \geqslant b \implies f(a) \geqslant f(b)$

D'où, par contraposition : $\quad f(a) < f(b) \implies a < b$

Exemple 3

Démontrer qu'il n'existe pas de fonction polynôme P tel que pour tout réel x :

$$P(x) = \mathbf{e}^x$$

Supposons qu'une telle fonction polynôme P existe. Notons n son degré.

En dérivant successivement $(n+1)$ fois, on obtiendrait, pour tout réel x :

$$0 = \mathbf{e}^x$$

Ce qui est absurde. Donc, l'exponentielle n'est pas une fonction polynomiale.

Exemple 4

Démontrer que $\sqrt{2}$ est irrationnel.

Supposons le contraire, on pourrait alors écrire $\sqrt{2}$ sous la forme de fraction irréductible[22].

Il existerait alors deux entiers a et b, premiers entre eux, tels que :

$$\sqrt{2} = \frac{a}{b}$$

On en déduit, par élévation au carré, une relation entre a et b :

$$a^2 = 2b^2$$

Donc a^2 serait un entier pair, et d'après l'exemple 1 ci-dessus, a également.

En conséquence, il existerait un entier k tel que $a = 2k$ et l'égalité ci-dessus deviendrait :

$$4k^2 = 2b^2$$

$$b^2 = 2k^2$$

Donc b^2, et par suite b, serait également un entier pair.

Ceci est en contradiction avec l'hypothèse que a et b sont premiers entre eux.

Donc $\sqrt{2}$ est irrationnel[23].

Raisonnement par contraposition

Démontrer une implication $p \Longrightarrow q$ équivaut, d'un point de vue logique, à démontrer $\text{non}(q) \Longrightarrow \text{non}(p)$:

$$(p \Longrightarrow q) \;\equiv\; \big(\text{non}(q) \Longrightarrow \text{non}(p)\big)$$

Raisonnement par l'absurde

- Démontrer une assertion p équivaut, d'un point de vue logique, à supposer sa négation $\text{non}(p)$ et aboutir à une contradiction :

  $$p \;\equiv\; \text{non}(p) \text{ absurde}$$

  Ou encore : $$p \;\equiv\; \text{non}\big(\text{non}(p)\big)$$

- Démontrer, sous une hypothèse p, que l'on a une assertion q équivaut, d'un point de vue logique, à supposer $\text{non}(q)$ et aboutir à une contradiction.

  $$(p \Longrightarrow q) \;\equiv\; \big(p \text{ et } \text{non}(q) \text{ absurde}\big)$$

  Ou encore : $$(p \Longrightarrow q) \;\equiv\; \text{non}\big(p \text{ et } \text{non}(q)\big)$$

22. Fraction du type $\frac{a}{b}$ où a et b sont des nombres entiers premiers entre eux, c'est-à-dire, sans autre diviseur commun que 1.

23. On verra à la page 146 une généralisation de ce résultat. Voir également à la page 36 pour une autre démonstration.

1.6 Un cas particulier de fonction : les suites

Définition 8 (Notion de suite)

Soit E un ensemble. On appelle *suite* toute fonction u de $\mathbb{N}$ dans E.

Une suite est généralement notée (u_n) où $n \in \mathbb{N}$.

Lorsque $E = \mathbb{Z}$, on dit que la suite est *entière*.

Lorsque $E = \mathbb{R}$, on dit que la suite est *réelle*.

Lorsque $E = \mathbb{C}$, on dit que la suite est *complexe*.

L'ensemble des suites à valeur dans un ensemble E est noté $E^{\mathbb{N}}$. En particulier, l'ensemble des suites réelles est noté $\mathbb{R}^{\mathbb{N}}$.

Une suite définie sur un intervalle $[\![m\,,n]\!]$ (où $m, n \in \mathbb{N}$ avec $m < n$) est dite *finie*.

Ne pas confondre, u_n qui désigne le terme[24] de rang n ($n \in \mathbb{N}$), (u_n) qui désigne la suite et $\{u_n\}$ qui est l'ensemble des éléments de la suite (ou l'image $u(\mathbb{N})$ de la fonction u).

Remarques

- Certaines suites ne sont définies qu'à partir d'un certain rang. C'est le cas, par exemple, de la suite (u_n) définie par $u_n = \sqrt{n-3}$ qui est définie pour $n \geqslant 3$.
- Certaines suites ne sont plus définies au delà d'un certain rang. C'est le cas, par exemple, de la suite (u_n) définie par $u_n = \sqrt{3-n}$ qui n'est plus définie pour $n \geqslant 4$. Plus subtilement, ceci peut également être le cas d'une suite définie par une relation de récurrence :
$$\begin{cases} u_0 & = & \frac{81}{80} \\ u_{n+1} & = & \frac{u_n}{3-2u_n} \end{cases}$$
On calcule alors $u_1 = \frac{27}{26}$, $u_2 = \frac{9}{8}$, $u_3 = \frac{3}{2}$ et pour $n \geqslant 4$, la suite n'est plus définie !
- Il n'existe pas que des suites numériques, on peut envisager des suites de polynômes, de fonctions, de matrices, etc.

24. Ce terme devrait logiquement se noter $u(n)$ mais l'usage en a voulu autrement. C'est à Lagrange (voir p. 489) que l'on doit la notation indicée u_n.

Définition 9

Soit (u_n) une suite de nombres réels définie au moins sur un intervalle I du type $[\![n_0\,,+\infty[\![$ (où $n_0 \in \mathbb{N}$)[25]. On dit que, à partir du rang n_0, la suite (u_n) est :

- *croissante* lorsque : $\forall n \in I,\ u_n \leqslant u_{n+1}$
- *strictement croissante* si : $\forall n \in I,\ u_n < u_{n+1}$
- *décroissante* lorsque : $\forall n \in I,\ u_n \geqslant u_{n+1}$
- *strictement décroissante* si : $\forall n \in I,\ u_n > u_{n+1}$
- *monotone* lorsqu'elle est croissante ou décroissante.
- *strictement monotone* en cas de stricte croissance ou stricte décroissance.
- *périodique* lorsque : $\exists T \in \mathbb{N}^*,\ \forall n \in I,\ u_{n+T} = u_n$

On dit que la suite (u_n) est :

- *constante* sur I lorsque : $\forall n \in I,\ u_n = u_{n+1}$
- *stationnaire* lorsque : $\exists n_1 \in I,\ \forall n \geqslant n_1,\ u_n = u_{n+1}$
- *majorée* lorsque : $\exists M \in \mathbb{R}, \forall n \in I,\ u_n \leqslant M$
- *minorée* lorsque : $\exists m \in \mathbb{R}, \forall n \in I,\ m \leqslant u_n$
- *bornée* lorsqu'elle est minorée et majorée :

$$\exists m, M \in \mathbb{R}, \forall n \in I,\ m \leqslant u_n \leqslant M$$

En particulier, une suite minorée (resp. majorée) par 0 est une suite positive (resp. négative).

À PARTIR D'UN CERTAIN RANG

Dire qu'une propriété $\mathcal{P}(n)$ s'applique à partir d'un certain rang N se code :

$$\exists N \in \mathbb{N}, \forall n \in \mathbb{N},\ \big(n \geqslant N \implies \mathcal{P}(n)\big)$$

Par exemple, dire qu'une suite (u_n) est positive à partir d'un certain rang se note :

$$\exists N \in \mathbb{N}, \forall n \in \mathbb{N},\ \big(n \geqslant N \implies u_n \geqslant 0\big)$$

Remarques

- Pour comprendre la nuance entre une suite stationnaire et une suite constante, donnons un exemple. Notons E la partie entière d'un réel (par exemple $E(\pi) = 3$) et (u_n) la

25. ou, à la rigueur, un intervalle du type $[\![n_0\,, m]\!]$ (où $n_0, m \in \mathbb{N}$ avec $n_0 < m$) dans le cas d'une suite finie.

suite définie, pour $n \in \mathbb{N}^*$, par :

$$u_n = E\left(\frac{1}{n}\right)$$

On a $u_1 = E(1) = 1$, $u_2 = E(0{,}5) = 0$ puis pour tout $n \geqslant 2$, $u_n = 0$. La suite (u_n) est stationnaire (à partir du rang 2) mais non constante puisque $u_1 = 1$ et $u_2 = 0$.

- Un exemple de suite périodique, à partir d'un certain rang, est la suite de Collatz[26] définie par un entier initial u_0 au choix et la relation de récurrence :

$$u_{n+1} = \begin{cases} \frac{u_n}{2} & \text{si} \quad u_n \text{ pair} \\ 3u_n + 1 & \text{si} \quad u_n \text{ impair} \end{cases}$$

  Par exemple, en choisissant $u_0 = 1$, on obtient successivement 4, 2, 1, 4, 2, 1, etc. Donc la suite est périodique (dès le début).

  Mais en choisissant $u_0 = 23$, on obtient successivement 70, 35, 106, 53, 160, 80, 40, 20, 10, 5, 16, 8, 4, 2, 1, 4, 2, 1 etc, et la suite est périodique à partir du rang 13.
- Il existe des suites qui sont ni croissantes, ni décroissantes. Par exemple : $u_n = (-1)^n$.
- Il est tout à fait correct de dire qu'une suite est croissante sur l'intervalle $[\![n_0\,,+\infty[\![$ au lieu de dire qu'elle est croissante à partir du rang n_0.
- Contrairement aux fonctions de la variable réelle, on ne définit le sens de variation d'une suite que sur des intervalles de la forme $[\![n_0\,,+\infty[\![$; ce qui se passe pour les premiers termes reste, ici, anecdotique.

Exemples

- Étudions le sens de variation de la suite (u_n) définie pour $n \in \mathbb{N}$ par :

$$u_n = \frac{n^2}{2^n}$$

  Calculons les premiers termes de cette suite et représentons-là graphiquement :

n	0	1	2	3	4	5
n^2	0	1	4	9	16	25
2^n	1	2	4	8	16	32
$\frac{n^2}{2^n}$	0	0,5	1	1,125	1	0,714

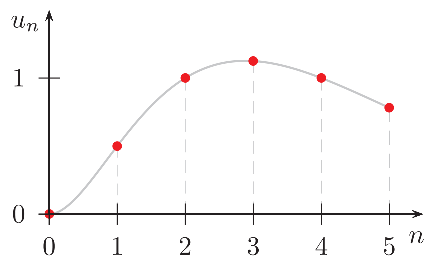


FIGURE 1.12 – La suite (u_n) définie par $u_n = \frac{n^2}{2^n}$.

26. Lothar Collatz, mathématicien allemand (1910-1990) émet, en 1937, la conjecture selon laquelle, quel que soit le choix de l'entier initial u_0, il existe un rang m pour lequel on a $u_m = 1$ (et donc $u_{m+1} = 4$, $u_{m+2} = 2$ et $u_{m+3} = 1 = u_m$) d'où la périodicité à partir d'un certain rang. Cette fameuse suite est, plus tard, étudiée de près à l'université de Syracuse (d'où la dénomination courante de « suite de Syracuse ») aux États-Unis. Aujourd'hui, on ne sait toujours pas prouver cette conjecture, vous pouvez chercher !

Cette suite semble décroissante pour $n \geqslant 3$.

En effet, étudions le signe de la différence de deux termes consécutifs[27] :

$$u_{n+1} - u_n = \frac{(n+1)^2}{2^{n+1}} - \frac{n^2}{2^n} = \frac{n^2}{2^{n+1}}\left(\frac{(n+1)^2}{n^2} - 2\right) = \frac{n^2}{2^{n+1}}\left(\left(1+\frac{1}{n}\right)^2 - 2\right)$$

Par ailleurs, on a :

$$n \geqslant 3 \iff \frac{1}{n} \leqslant \frac{1}{3} \iff 1 + \frac{1}{n} \leqslant \frac{4}{3} \iff \left(1+\frac{1}{n}\right)^2 \leqslant \frac{16}{9}$$

Et comme $\frac{16}{9} < 2$, on a au final :

$$u_{n+1} - u_n < 0 \iff n \geqslant 3$$

La suite (u_n) est bien décroissante pour $n \geqslant 3$.

Notons, au passage, que cette suite (u_n) est majorée par $\frac{9}{8}$.

- **Important** : considérons la suite (u_n) définie pour $n \in \mathbb{N}^*$ par :

$$u_n = \sum_{k=1}^{n} \frac{1}{k^2}$$

Montrons que cette suite est majorée.

Pour tout $k \geqslant 2$, on a : $\quad \dfrac{1}{k^2} \leqslant \dfrac{1}{k(k-1)} \leqslant \dfrac{1}{k-1} - \dfrac{1}{k}$

Ainsi, pour $n \geqslant 2$, on obtient par télescopage :

$$u_n = 1 + \sum_{k=2}^{n} \frac{1}{k^2} \leqslant 1 + \sum_{k=2}^{n}\left(\frac{1}{k-1} - \frac{1}{k}\right) \leqslant 1 + 1 - \frac{1}{n} \leqslant 2 - \frac{1}{n} \leqslant 2$$

Cette suite est bien majorée[28] par 2.

1.7 Propriétés de $\mathbb{N}$ (et $\mathbb{Z}$). Récurrence

Plusieurs options sont possibles pour construire l'ensemble des entiers naturels $\mathbb{N}$.

Mais toute construction mathématique repose sur un choix d'axiomes.

Axiome 1

Toute partie non vide de $\mathbb{N}$ admet un plus petit élément[29].

27. Pour une suite dont les termes sont tous strictement positifs, on peut remarquer via la relation $u_{n+1} - u_n = u_n\left(\frac{u_{n+1}}{u_n} - 1\right)$ qu'étudier le signe de la différence de deux termes consécutifs équivaut à comparer le quotient $\frac{u_{n+1}}{u_n}$ à 1.

28. Cette majoration était déjà connue de Jacques Bernoulli (1654-1705, voir page 565). Dans *Positiones arithmeticae de seriebus infinitis, earumque summa finita*, Basileae (1689), il s'intéresse à cette série mais il n'arrive pas à calculer la somme dont il reconnaît qu'elle est difficile à déterminer (cf. *ibid.* p. 399). Il faudra attendre Euler en 1734 qui démontre que la somme vaut $\frac{\pi^2}{6}$ (voir exercice page 745).

29. On admet qu'il y a un ordre « naturel » $\leqslant$ sur $\mathbb{N}$ et qu'un plus petit élément m d'une partie A de $\mathbb{N}$ est défini par $m \leqslant a$ quel que soit l'élément a de A. Notons que l'on a nécessairement $m \in A$.

Exemple

Considérons l'ensemble A des entiers naturels ayant exactement cinq diviseurs. Cet ensemble est non vide (par exemple $81 \in A$ puisque 81 possède cinq diviseurs qui sont 1, 3, 9, 27 et 81). D'après l'axiome ci-dessus, cet ensemble admet donc un plus petit élément. On vérifie facilement qu'il s'agit du nombre $2^4 = 16$.

Le choix de l'axiome ci-dessus[30] nous permettra de faire une démonstration du principe de raisonnement par récurrence. Mais avant d'en venir à la récurrence voyons une application sympathique de cet axiome.

Application : une démonstration, par l'absurde, de l'irrationalité[31],[32]de $\sqrt{2}$

Supposons que $\sqrt{2}$ soit un nombre rationnel. Cela signifie qu'il existerait une fraction $\frac{a}{b}$ d'entiers tels que :

$$\sqrt{2} = \frac{a}{b}$$

Autrement dit, il existerait un certain multiple de $\sqrt{2}$ qui serait un entier (ici $b\sqrt{2}$). Considérons alors l'ensemble A des entiers non nuls n tels que $n\sqrt{2}$ soit un entier :

$$A = \left\{ n \in \mathbb{N}^*, \text{ tels que } n\sqrt{2} \in \mathbb{N}^* \right\}$$

Par hypothèse, cet ensemble A est une partie **non vide** de $\mathbb{N}^*$ (et donc de $\mathbb{N}$) puisqu'il contient b. D'après l'axiome ci-dessus, il admet un **plus petit élément** m (avec $m \in \mathbb{N}^*$). Considérons alors le nombre m' défini par :

$$m' = m\sqrt{2} - m$$

Nous pouvons dire plusieurs choses intéressantes sur ce nombre m'.

- D'une part : $\boldsymbol{m' \in \mathbb{N}^*}$. En effet, par hypothèse, $m\sqrt{2}$ est un entier donc $m' = m\sqrt{2} - m$ également. Et il est non nul car s'il l'était, on aurait $\sqrt{2} = 1$ ce qui est absurde (il suffit d'élever au carré pour s'en convaincre).
- D'autre part : $\boldsymbol{m' \in A}$. En effet :

  $$m'\sqrt{2} = \left(m\sqrt{2} - m\right)\sqrt{2} = 2m - \sqrt{2}m$$

  Or $2m$ est un entier, $\sqrt{2}m$ aussi par hypothèse donc $2m - \sqrt{2}m$ également. Et ce dernier entier est non nul car s'il l'était, on aurait $\sqrt{2} = 2$ ce qui est absurde (là encore, il suffit d'élever au carré pour s'en convaincre).

30. D'autres choix sont possibles, on peut notamment inclure le principe de récurrence dans l'axiomatique permettant de construire $\mathbb{N}$ comme l'a fait le mathématicien Guiseppe Peano (1858-1932) dans son ouvrage *Arithmetices principia, nova methodo exposita* publié en 1889.
31. Un nombre est dit *irrationnel* lorsqu'il n'est pas rationnel, autrement dit, lorsqu'il ne peut pas s'exprimer sous forme de fraction de nombres entiers.
32. Voir également à la page 146 pour une démonstration classique (et généralisée) de ce résultat.

- Et enfin : $\boldsymbol{m' < m}$. En effet, on a $m' = m(\sqrt{2}-1)$. Or, $\sqrt{2}-1$ est inférieur à 1 (si on avait $\sqrt{2}-1 \geqslant 1$, on aurait $\sqrt{2} \geqslant 2$ ce qui est absurde, il suffit d'utiliser la croissance de la fonction « carré » sur $\mathbb{R}_+$ pour s'en convaincre).

Nous avons donc une contradiction puisqu'on a trouvé, dans A, un élément m' strictement inférieur à l'élément m qui était censé être le plus petit. On en déduit que $\sqrt{2}$ est un nombre irrationnel.

Venons-en maintenant au **principe de raisonnement par récurrence** que nous allons introduire à l'aide de trois exemples simples.

Exemple 1

Considérons la suite (u_n), définie pour tout $n \in \mathbb{N}$, par :

$$\begin{cases} u_0 & = & 0 \\ u_{n+1} & = & 2u_n + 1 \end{cases}$$

Cette suite est définie par récurrence (chaque terme depend du précédent). On souhaiterait obtenir une formule permettant de calculer explicitement chaque terme u_n en fonction de n. À premiere vue, cette formule ne saute pas aux yeux. Dans une telle situation, le calcul des premiers termes est souvent intéressant pour se faire une « idée ».

Ici, nous avons :

$$u_1 = 2u_0 + 1 = 1$$

$$u_2 = 2u_1 + 1 = 3$$

$$u_3 = 2u_2 + 1 = 7$$

$$u_4 = 2u_3 + 1 = 15$$

$$u_5 = 2u_4 + 1 = 31$$

Stop, nous remarquons que la suite (u_n) semble obéir à une loi toute simple : en ajoutant 1 à chaque terme, on obtient les puissances successives de 2.

Nous pouvons donc émettre la conjecture suivante :

$$\forall n \in \mathbb{N},\ u_n = 2^n - 1$$

Attention, une conjecture n'est pas une preuve (ni une affirmation forcément vraie, certaines conjectures se révèlent parfois fausses...). Ce n'est que l'énoncé d'une propriété resultant d'un certain nombre d'observations.

Alors comment confirmer, par une démonstration, la propriété conjecturée ci-dessus ?

Notons $\mathcal{P}$ la propriété[33], définie pour $n \in \mathbb{N}$ par :

$$\mathcal{P}(n) : u_n = 2^n - 1$$

Supposons, un instant, que pour un certain entier n, on ait effectivement la propriété $\mathcal{P}(n) : u_n = 2^n - 1$ qui est satisfaite. Alors, sous cette condition, on aurait :

$$u_{n+1} = 2u_n + 1 = 2(2^n - 1) + 1 = 2^{n+1} - 1$$

Ce qui correspond à l'énoncé de $\mathcal{P}(n+1)$.
Autrement dit, si la propriété est vraie à un certain rang n, alors elle l'est également au rang suivant. On dit que la propriété $\mathcal{P}$ est *héréditaire*.
Faisons un bilan : on a vérifié que la propriété $\mathcal{P}$ est vraie aux rangs $n = 0\,,1\,,2\,,3\,,4$ et 5. On dit que la propriété $\mathcal{P}$ est *initialisée*. Mais comme elle est héréditaire, elle sera vraie encore au rang $n = 6$, puis au rang $n = 7$, etc. Si bien que notre propriété est finalement vraie à tout rang.
Nous venons de faire un raisonnement par récurrence :

Principe de raisonnement par récurrence (simple)[34]

Soit $\mathcal{P}$ une propriété définie sur $\mathbb{N}$.
$\boxed{\text{SI}}$:

- la propriété $\mathcal{P}$ est INITIALISÉE à un certain rang n_0, c'est-à-dire :

$$\mathcal{P}(n_0) \text{ est vraie}^{35}$$

- la propriété $\mathcal{P}$ est HÉRÉDITAIRE à partir du rang n_0, c'est-à-dire :

$$\text{pour tout entier } n \geqslant n_0,\ \Big(\mathcal{P}(n) \implies \mathcal{P}(n+1)\Big)$$

$\boxed{\text{ALORS}}$:La propriété $\mathcal{P}$ est vraie à tout rang n plus grand que n_0.

33. Il s'agit, en fait, d'une *famille* de propriétés.
34. On trouve des traces du raisonnement par récurrence dans les *Éléments* d'Euclide (voir page 109) qui affirmait : *nous avons vérifié la propriété pour 2, nous avons montré que si elle est vraie pour un nombre, elle est vraie pour son suivant, donc elle est générale*. Plus tard, Blaise Pascal (voir page 68) l'utilise explicitement dans son *Traité du triangle arithmétique* écrit en 1654 et publié en 1665 en l'appelant « raisonnement par induction ». Les anglo-saxons utilisent le terme « *mathematical induction* » et attribuent souvent à De Morgan, en 1838, la paternité du vocable (De Morgan rédige un effet une entrée dans l'encyclopédie *The Penny Cyclopaedia* de la Society for the Diffusion of Useful Knowledge, **12**). Mais c'est oublier les contributions de leur compatriote John Wallis (voir page 697) qui, en 1656, utilise l'expression « *per modum inductionis* » dans son livre *Arithmetica Infinitorum*, page 15, proposition XIX. En 1861, dans son livre *Lehrbuch der Mathematik für höhere Lehranstalten* le mathématicien allemand Hermann Grassmann (1809-1877) donne la formulation moderne de ce principe telle qu'elle est utilisée aujourd'hui. Quant au terme francisé de « récurrence », il semble apparaître assez tardivement, il est employé en 1902 par Henri Poincaré dans le chapitre 1 de *La science de l'hypothèse*.
35. On peut se contenter de dire « $\mathcal{P}(n_0)$ » au lieu de « $\mathcal{P}(n_0)$ est vraie ». Qui dit, au quotidien, lorsqu'il pleut : « il pleut est vrai » au lieu de « il pleut » ! ?

Exemple 2

Voyons ici une propriété qui n'est initialisée qu'à partir d'un certain rang.

Comparons les valeurs de $n!$[36] avec les puissances successives de 2.

n	0	1	2	3	4	5
2^n	1	2	4	8	16	32
$n!$	1	1	2	6	24	120

On ne peut pas affirmer que $n!$ est supérieur à 2^n pour tout entier naturel n. Il semble cependant que ce soit le cas pour $n \geqslant 4$. Nous allons le démontrer par récurrence en considérant la propriété suivante :

$$\mathcal{P}(n) : n! \geqslant 2^n$$

- Puisque $4! \geqslant 2^4$, on a $\mathcal{P}(4)$. Ici, la propriété est initialisée au rang 4.
- Soit $n \geqslant 4$ et supposons $\mathcal{P}(n)$. Alors, on peut écrire :

$$(n+1)! \geqslant (n+1) \times n! \overset{\mathcal{P}(n)}{\geqslant} (n+1) \times 2^n \overset{n \geqslant 4}{\geqslant} 2 \times 2^n \geqslant 2^{n+1}$$

  Ce qui correspond à $\mathcal{P}(n+1)$.

  La propriété $\mathcal{P}$ est donc héréditaire à partir du rang 4.

Bilan : on a montré : $\mathcal{P}(4)$ et $\Big(\forall n \geqslant 4, \, \mathcal{P}(n) \implies \mathcal{P}(n+1)\Big)$

Du principe de raisonnement par récurrence, on en déduit $\mathcal{P}(n)$ pour tout entier $n \geqslant 4$.

Notons que l'on peut également démontrer (en traitant le cas $n = 0$ à part) que :

$$\forall n \in \mathbb{N}, \, n! \geqslant 2^{n-1}$$

Exemple 3

Et enfin, voici un dernier exemple où l'on fait une récurrence **finie**.[37]

Soit $n \in \mathbb{N}^*$.

1. Démontrer que : $\forall m \in [\![1\,,n]\!], \, \left(1 + \dfrac{1}{n}\right)^m < 1 + \dfrac{m}{n} + \left(\dfrac{m}{n}\right)^2$

2. En déduire que $\left(1 + \dfrac{1}{n}\right)^n < 3$.

Dans cet exemple, nous n'aurons besoin de l'hérédité que pour un nombre fini d'étapes.

1. Ici, on considère donc, fort logiquement, la propriété $\mathcal{P}$ définie pour $m \in [\![1\,,n]\!]$ par :

$$\mathcal{P}(m) : \left(1 + \frac{1}{n}\right)^m < 1 + \frac{m}{n} + \left(\frac{m}{n}\right)^2$$

36. On rappelle que *la factorielle* d'un entier n, notée $n!$, est définie par $0! = 1$ et, pour $n \in \mathbb{N}^*$ par le produit $n! = 1 \times 2 \times \cdots \times n$. Par exemple $4! = 1 \times 2 \times 3 \times 4 = 24$. On convient que $0! = 1$. Petite curiosité : démontrer que $10! = 6! \times 7!$.
La notation $n!$ est introduite par le mathématicien français Christian Kramp en 1808 dans son livre *Éléments d'arithmétique universelle*.

37. Voir par exemple l'exercice 1.16 (page 139) pour un autre exemple de récurrence finie ou encore la démonstration de la formule de Leibniz, page 483.

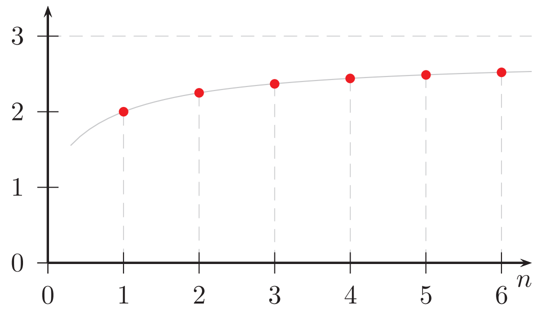


FIGURE 1.13 – Suite majorée par 3.

- Lorsque $m = 1$, on a bien $1 + \frac{1}{n} < 1 + \frac{1}{n} + \frac{1}{n^2}$ d'où $\mathcal{P}(1)$.

  Si $n = 1$, alors la question est terminée. Supposons désormais $n \geqslant 2$.
- Soit $m \in [\![1\,,n-1]\!]$ et supposons $\mathcal{P}(m)$.

  On peut alors écrire :
$$\left(1+\frac{1}{n}\right)^{m+1} < \left(1+\frac{m}{n}+\left(\frac{m}{n}\right)^2\right)\left(1+\frac{1}{n}\right)$$
  En développant le membre de droite :
$$\left(1+\frac{1}{n}\right)^{m+1} < 1+\frac{1}{n}+\frac{m}{n}+\frac{m}{n^2}+\frac{m^2}{n^2}+\frac{m^2}{n^3}$$
  Or $0 < m < n$ donc $m^2 < mn$ et on peut majorer le dernier terme $\frac{m^2}{n^3}$ par $\frac{m}{n^2}$.

  D'où : $\left(1+\frac{1}{n}\right)^{m+1} < 1+\frac{m+1}{n}+\frac{m^2+2m}{n^2} < 1+\frac{m+1}{n}+\frac{(m+1)^2}{n^2}$

  Ce qui est $\mathcal{P}(m+1)$.

On a montré : $\mathcal{P}(1)$ et $\Big(\forall m \in [\![1\,,n-1]\!],\, \mathcal{P}(m) \implies \mathcal{P}(m+1)\Big)$

On en déduit : $\forall m \in [\![1\,,n]\!],\, \mathcal{P}(m)$

D'où le résultat.

2. Il suffit de spécialiser $m = n$ pour obtenir :
$$\left(1+\frac{1}{n}\right)^{n} < 3$$
Remarquons que l'on peut obtenir une majoration bien meilleure à l'aide de l'inégalité $\ln(1+x) \leqslant x$ (voir page 94) spécialisée avec $x = \frac{1}{n}$:
$$\ln\left(1+\frac{1}{n}\right) \leqslant \frac{1}{n}$$
$$n\ln\left(1+\frac{1}{n}\right) \leqslant 1$$

Par propriétés du logarithme : $\quad \ln\left(\left(1+\frac{1}{n}\right)^n\right) \leqslant 1$

Puis, par croissance de la fonction exponentielle sur $\mathbb{R}$, on obtient[38] :

$$\left(1+\frac{1}{n}\right)^n \leqslant \mathbf{e}$$

Donnons maintenant un énoncé précis et rigoureux du principe de raisonnement par récurrence (qui englobe toutes les formes de récurrence : finie, forte, à partir d'un certain rang).

Théorème 4 (Principe de raisonnement par récurrence)

Soit I un intervalle[39] de $\mathbb{N}$, non réduit à un singleton.

Soit $\mathcal{P}$ une propriété définie sur I.

$\boxed{\text{SI}}$ les deux conditions suivantes sont satisfaites :

- Initialisation : $\quad \exists n_0 \in I$ tel que $\mathcal{P}(n_0)$
- Hérédité : $\forall n \in I \cap [\![n_0\,,+\infty[\![$ tel que $n+1 \in I$: $\mathcal{P}(n) \Longrightarrow \mathcal{P}(n+1)$

$\boxed{\text{ALORS :}}$ $\quad \forall n \in I \cap [\![n_0\,,+\infty[\![,\ \mathcal{P}(n)$

Démonstration

Considérons l'ensemble E des entiers naturels inclus dans I et supérieurs à n_0 pour lesquels la propriété $\mathcal{P}$ n'est pas satisfaite :

$$E = \left\{n \in I \cap [\![n_0\,,+\infty[\![,\ \text{non}\big(\mathcal{P}(n)\big)\right\}$$

Raisonnons par l'absurde en supposant E non vide. D'après l'axiome 1, page 35, cet ensemble E admet alors un plus petit élément m (supérieur à n_0).

Comme ce plus petit élément m est élément de E, on a donc $\text{non}\big(\mathcal{P}(m)\big)$.

- Si $m = n_0$, alors on a $\text{non}\big(\mathcal{P}(n_0)\big)$ ce qui contredit l'hypothèse d'initialisation.
- Si $m > n_0$, alors on a, du fait que m est le plus petit élément de E :

$$\mathcal{P}(m-1) \text{ et } \text{non}\big(\mathcal{P}(m)\big)$$

  ce qui contredit l'hypothèse d'hérédité.

En conséquence, E est vide, autrement dit :

$$\forall n \in I \cap [\![n_0\,,+\infty[\![,\ \mathcal{P}(n)$$

38. Ainsi, si l'expression $\left(1+\frac{1}{n}\right)^n$ admet une limite lorsque n tend vers l'infini, cette limite est nécessairement inférieure ou égale à 3 et même à $\mathbf{e}$. L'existence et la valeur de cette limite seront précisées à la page 315.

39. Les intervalles de $\mathbb{N}$ sont les ensembles du type $[\![a\,,b]\!]$ (ensemble des entiers compris entre les entiers a et b) ou du type $[\![a\,,+\infty[\![$ (ensemble des entiers supérieurs à l'entier a).

Le principe de récurrence étant démontré, nous pouvons donner maintenant un corollaire important de l'axiome 1, page 35.

Corollaire 1

1. Toute partie non vide et majorée[40] de $\mathbb{N}$ admet un plus grand élément.

2. Toute partie non vide et majorée de $\mathbb{Z}$ admet un plus grand élément.

Démonstration

1. Considérons la propriété suivante :

$$\mathcal{P}(n) : \text{ toute partie non vide de } \mathbb{N} \text{ et majorée par } n \text{ admet un plus grand élément.}$$

- Si une partie de $\mathbb{N}$ majorée par 0, c'est qu'elle est nécessairement réduite au singleton $\{0\}$. Elle admet donc un plus grand élément qui est 0 d'où $\mathcal{P}(0)$.
- Soit $n \in \mathbb{N}$ et supposons $\mathcal{P}(n)$.
  Considérons alors une partie A de $\mathbb{N}$ non vide et majorée par $n+1$.
  - Si n majore A alors, d'après $\mathcal{P}(n)$, la partie A admet un plus grand élément.
  - Si n ne majore pas A alors il existe dans A un élément strictement supérieur à n. Mais par ailleurs, cet élément est nécessairement inférieur ou égal à $n+1$ qui, par hypothèse, majore A donc cet élément est bien $n+1$. On a un majorant (à savoir $n+1$) qui est dans A donc $n+1$ est le plus grand élément de A.

  Dans tous les cas, on obtient $\mathcal{P}(n+1)$.

On a donc montré : $\quad \mathcal{P}(0)$ et $\Big(\forall n \in \mathbb{N},\, \mathcal{P}(n) \Longrightarrow \mathcal{P}(n+1)\Big)$

Du principe de raisonnement par récurrence, on en déduit : $\forall n \in \mathbb{N},\, \mathcal{P}(n)$.

Bilan : si on se donne une partie non vide et majorée de $\mathbb{N}$, d'après ce qu'on vient de voir, en notant n son majorant, cette partie admet un plus grand élément.

2. Soit A une partie non vide et majorée de $\mathbb{Z}$.

- Si $A \cap \mathbb{N} = \varnothing$ alors A est majorée par 0.
  On pose alors $B = -A = \{-x \text{ où } x \in A\}$.
  Ainsi B est une partie non vide de $\mathbb{N}$ donc admet un plus petit élément m, ce qui signifie :

$$m \in B \text{ et } \forall b \in B, m \leqslant b$$

  Mais les éléments b de B peuvent tous s'écrire $b = -x$ où x parcourt A, ainsi :

$$-m \in A \text{ et } \forall x \in A, m \leqslant -x$$

40. Une partie A de $\mathbb{N}$ (ou $\mathbb{Z}$) est majorée s'il existe un entier M tel que : $\forall a \in A, a \leqslant M$. Notons que M n'est pas nécessairement élément de A. Par exemple, la partie $A = \{1\,,2\,,3\}$ est majorée par 3 mais aussi par 4 ou 5.

$$-m \in A \text{ et } \forall x \in A, x \leqslant -m$$

Ce qui prouve que A admet un plus grand élément (à savoir $-m$).

- Si $A \cap \mathbb{N} \neq \varnothing$ alors l'ensemble $A \cap \mathbb{N}$ est une partie non vide de $\mathbb{N}$ et majorée dans $\mathbb{N}$ donc d'après le point précédent admet un plus grand élément N qui, *a fortiori*, est également le plus grand élément de A.

1.8 Injection, surjection, bijection

Définition 10 (Injection, surjection, bijection)
Soit $f : E \longrightarrow F$ une application. On dit que :

- f est *injective* lorsque deux éléments distincts ont des images distinctes[41] :
$$\forall x_1, x_2 \in E, \ \big(f(x_1) = f(x_2) \implies x_1 = x_2\big)$$
- f est *surjective* lorsque tout élément y de F admet au moins un antécédent :
$$\forall y \in F, \exists x \in E, \ y = f(x)$$
- f est *bijective* lorsqu'elle est injective et surjective.

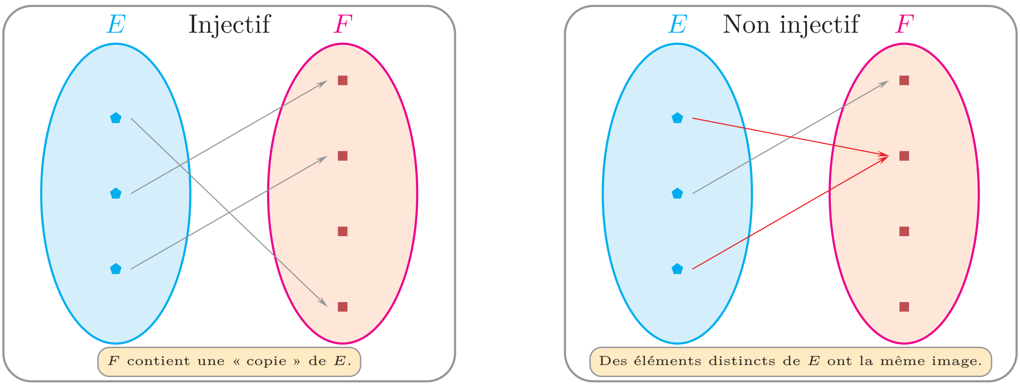


FIGURE 1.14 – Concept d'injection.

Exemples

- L'application :
$$\begin{array}{rccc} f : & \mathbb{R} & \longrightarrow & \mathbb{R}_+ \\ & x & \longmapsto & x^2 \end{array}$$
n'est pas injective puisque deux nombres opposés ont la même image.

41. Cela signifie $x_1 \neq x_2 \implies f(x_1) \neq f(x_2)$. Mais dans la pratique, l'implication contraposée (voir page 31) proposée dans la définition est, dans de nombreux cas, plus aisée à vérifier.

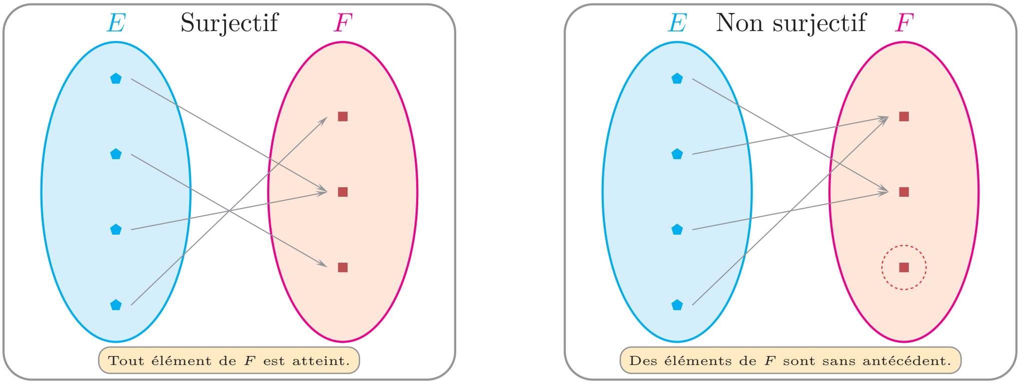


FIGURE 1.15 – Concept de surjection.

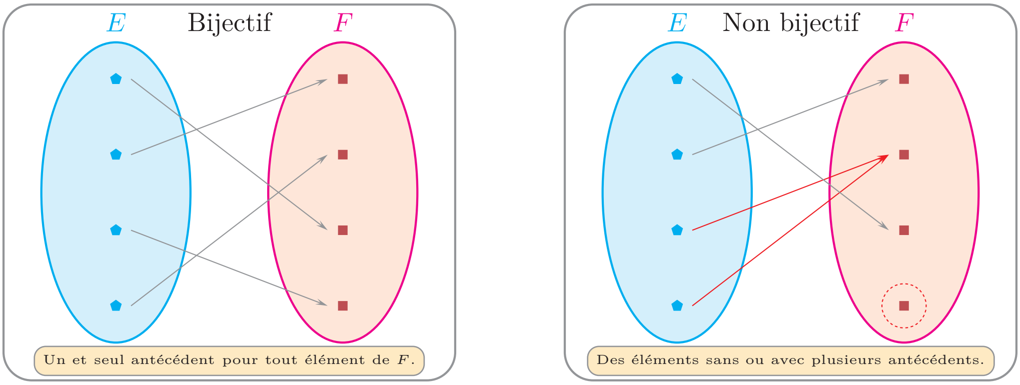


FIGURE 1.16 – Concept de bijection.

En revanche, elle est surjective puisque pour tout réel y positif, on peut trouver au moins un réel x tel que $y = x^2$, par exemple $\sqrt{y}$.

- L'application : $$\begin{array}{rccc} f: & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & n & \longmapsto & n^2 \end{array}$$

est injective. En effet, supposons qu'il existe deux entiers naturels n_1 et n_2 tels que :

$$f(n_1) = f(n_2)$$

$$n_1^2 = n_2^2$$

$$(n_1 - n_2)(n_1 + n_2) = 0$$

$$n_1 = n_2 \text{ ou } n_1 + n_2 = 0$$

Mais, comme n_1 et n_2 sont des entiers naturels, la condition $n_1 + n_2 = 0$ entraîne $n_1 = n_2 = 0$. Dans tous les cas, on a $n_1 = n_2$ d'où l'injectivité de l'application f.

En revanche, cette application n'est pas surjective puisqu'il existe des éléments de l'ensemble d'arrivée (par exemple 2 ou 3) qui n'ont pas d'antécédent dans $\mathbb{N}$.

- Soit $f : I \longrightarrow \mathbb{R}$ une fonction strictement croissante sur un intervalle I. Alors f est nécessairement injective. En effet, si x_1 et x_2 sont deux éléments distincts, on a $x_1 < x_2$ ou $x_1 > x_2$, mais par stricte croissance de f, ceci implique $f(x_1) < f(x_2)$ ou $f(x_1) > f(x_2)$ donc $f(x_1) \neq f(x_2)$.

  Il en est de même pour une fonction $f : I \longrightarrow \mathbb{R}$ strictement décroissante.
- L'application : $$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{R}_+^* \\ & x & \longmapsto & \mathbf{e}^x \end{array}$$

  est bijective puisque d'une part $\mathbf{e}^x = \mathbf{e}^y \implies x = y$ d'où l'injectivité et d'autre part, pour tout $y \in \mathbb{R}_+^*$, il existe $x \in \mathbb{R}$ tel que $y = \mathbf{e}^x$, à savoir $x = \ln(y)$, d'où la surjectivité. On renvoie le lecteur à la page 581 pour une construction rigoureuse de la fonction exponentielle.

Remarques

- La restriction d'une injection $f : E \longrightarrow F$ à une partie $E' \subseteq E$ reste une injection. La restriction se note $f_{|E'}$.
- Toute application $f : E \longrightarrow F$ peut être « rendue » surjective en restreignant l'ensemble d'arrivée à $f(E)$. Une telle opération est parfois appelée *corestriction* et est notée $f^{|f(E)}$.
- La surjectivité d'une application $f : E \longrightarrow F$ assure au moins un antécédent à tout élément y de l'ensemble F. Si, de plus, f est injective, y ne peut avoir plusieurs antécédents. En conséquence, on a une nouvelle formulation pratique de la bijectivité :

$$\boxed{f : E \longrightarrow F \text{ est bijective } \iff \forall y \in F, \exists! x \in E,\ y = f(x)}$$

Théorème 5 (Composition d'injections, de surjections et de bijections)

La composée[42] de deux injections est une injection.

La composée de deux surjections est une surjection.

La composée de deux bijections est une bijection.

Démonstration

Soient E, F et G trois ensembles.

Soit f une application de E dans F et g une application de F dans G.

42. La composée (ou la composition) de deux applications $f : E \longrightarrow F$ suivie de $g : F \longrightarrow G$, notée $g \circ f$ est l'application :

$$\begin{array}{rccc} g \circ f: & E & \longrightarrow & G \\ & x & \longmapsto & g\big(f(x)\big) \end{array}$$

En général $g \circ f \neq f \circ g$.

Supposons f et g injectives. Montrons que $g \circ f$ l'est également.

Soient z_1 et z_2 deux éléments de G tels que :

$$g \circ f(z_1) = g \circ f(z_2)$$

Mais puisque g est injective : $\qquad f(z_1) = f(z_2)$

Et comme f l'est également : $\qquad z_1 = z_2$

D'où l'injectivité de $g \circ f$.

Supposons f et g surjectives. Montrons que $g \circ f$ l'est également.

Soit z un élément de G.

Comme g est surjective, il existe y dans F tel que $g(y) = z$.

Mais comme f est surjective, il existe x dans E tel que $f(x) = y$.

Ainsi, on a $g \circ f(x) = z$ ce qui prouve la surjectivité de $g \circ f$.

Supposons f et g bijectives.

Alors f et g sont à la fois des injections et des surjections.

Mais d'après ce qui précède, on en déduit que $g \circ f$ est injective et surjective.

Ce qui, par définition, permet de conclure que $g \circ f$ est bijective.

Définition 11 (Bijection réciproque)

Soit $f : E \longrightarrow F$ une application bijective.

L'application, notée f^{-1}, qui à tout élément y de F associe son unique antécédent x dans E, est appelée la *bijection réciproque* de f.

En conséquence, la bijection réciproque f^{-1} de f est bien bijective (ouf !) et on a :

$$\left(f^{-1}\right)^{-1} = f \text{ et } \begin{cases} f^{-1} \circ f = Id_E \\ f \circ f^{-1} = Id_F \end{cases}$$

Notons que si f est une surjection de E dans F et s'il existe une application g de F dans E telle que $g \circ f = Id_E$ alors f est bijective et $g = f^{-1}$.

En effet, soit $x \in E$. Notons x' un antécédent de $f(x)$. On a donc $f(x') = f(x)$ et en composant par g :

$$g \circ f(x') = g \circ f(x)$$

Et comme, par hypothèse $g \circ f = Id_E$, on en déduit $x' = x$ donc f est injective et donc, par suite, bijective. De plus, si on note $y = f(x)$, on a $g(y) = g\big(f(x)\big) = x$ donc g envoie y sur x, on a donc bien $g = f^{-1}$.

Exemple

Soit f la fonction définie pour tout $x \in \mathbb{R}_+$ par :

$$f(x) = \frac{x}{1+x}$$

Montrons que f réalise une bijection de $\mathbb{R}_+$ sur un ensemble que l'on précisera et déterminons sa bijection réciproque.

Des inégalités $0 \leqslant x < x+1$, on déduit facilement $0 \leqslant f(x) < 1$. Donc $f(\mathbb{R}_+) \subseteq [0\,,1[$.

Soit $y \in [0\,,1[$. Cherchons s'il existe un réel positif x tel que $f(x) = y$ *i.e.* :

$$\frac{x}{1+x} = y$$

$$x = y(1+x) = y + xy$$

$$x(1-y) = y$$

Et comme $y \neq 1$, on en déduit : $\quad x = \dfrac{y}{1-y}$

Ainsi, tout élément y de l'ensemble d'arrivée admet un unique antécédent x dans $\mathbb{R}_+$.

On en déduit que la fonction f réalise une bijection de $\mathbb{R}_+$ dans $[0\,,1[$.

On obtient une expression de la bijection réciproque en permutant les rôles de x et y :

$$\begin{array}{rccc} f^{-1}: & [0\,,1[& \longrightarrow & \mathbb{R}_+ \\ & x & \longmapsto & \frac{x}{1-x} \end{array}$$

On peut vérifier que, pour tout $x \in \mathbb{R}_+$, on a :

$$f^{-1} \circ f(x) = f^{-1}\left(\frac{x}{1+x}\right) = \frac{\frac{x}{1+x}}{1 - \frac{x}{1+x}} = \frac{\frac{x}{1+x}}{\frac{1+x-x}{1+x}} = x$$

On vérifie, de même, que pour tout $x \in [0\,,1[$, on a $f \circ f^{-1}(x) = x$.

Du fait du rôle permuté des images et antécédents entre bijection et bijection réciproque, les représentations graphiques de f de f^{-1} sont symétriques par rapport à la « première diagonale » $\Delta : y = x$.

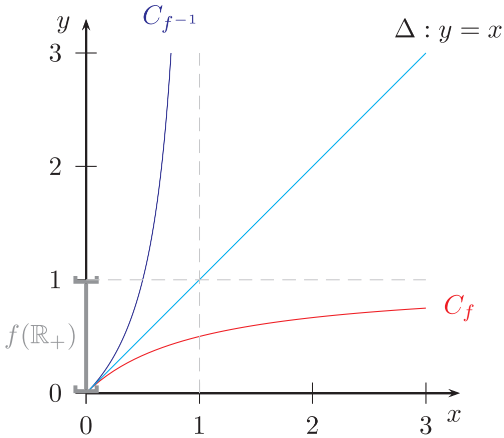


Figure 1.17 – Une bijection (de $\mathbb{R}_+$ dans $[0\,,1[$) et sa réciproque.

1.9 Cardinaux

On a envie de dire que le cardinal d'un ensemble est son nombre d'éléments. Nous savons que, lorsque $n \in \mathbb{N}^*$, l'ensemble $[\![1\,,n]\!]$ contient n éléments mais quel est, par exemple, le nombre d'éléments de l'ensemble $\mathcal{P}(E)$ des parties d'un ensemble E ? Comment dénombrer ces éléments tout en étant sûr de ne pas en avoir oublié ? Ces notions ne sont pas aussi évidentes qu'on pourrait le croire et nous allons, ici, définir la notion de cardinal d'un ensemble à partir du concept de bijection. Ainsi, si on trouve une bijection entre un ensemble E et l'ensemble $[\![1\,,n]\!]$, nous pourrons affirmer que l'ensemble E en question possède exactement n éléments. À condition de s'être bien assuré que si un tel entier n existe, il est unique...

1.9.1 Vers la notion de cardinal - Compléments[43]

Nous aurons besoin, dans un premier temps, de quelques petits lemmes préalables ne faisant intervenir que des ensembles de référence du type $[\![1\,,n]\!]$.

Lemme 1

Soit $n \in \mathbb{N} \setminus \{0\,,1\}$. Soit $e \in [\![1\,,n]\!]$.

Il existe une bijection entre $[\![1\,,n-1]\!]$ et $[\![1\,,n]\!] \setminus \{e\}$.

Ce que dit ce lemme est tout simple : si on enlève un élément e à $[\![1\,,n]\!]$, on pourra toujours mettre l'ensemble obtenu en bijection avec $[\![1\,,n-1]\!]$. Mais pour prouver cette « évidence », nous nous devons d'« exhiber » la bijection !

Démonstration

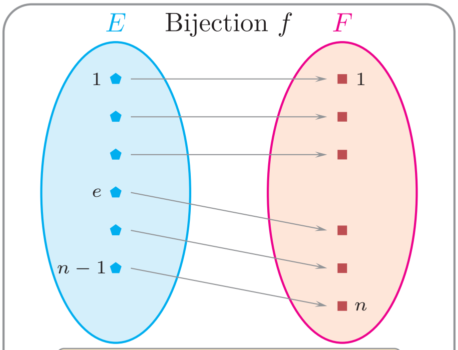
Considérons l'application f définie par :

$$\begin{array}{rccl} f: & [\![1\,,n-1]\!] & \longrightarrow & [\![1\,,n]\!] \setminus \{e\} \\ & m & \longmapsto & f(m) = \left\{\begin{array}{ccc} m & \text{si} & 1 \leqslant m < e \\ m+1 & \text{si} & e \leqslant m \leqslant n-1 \end{array}\right. \end{array}$$

Cette application est bien définie, puisque pour tout m de $[\![1\,,n-1]\!]$, on aura bien $f(m) \in [\![1\,,n]\!] \setminus \{e\}$.

Notons, pour la suite de la démonstration $E = [\![1\,,n-1]\!]$ et $F = [\![1\,,n]\!] \setminus \{e\}$.

43. Cette partie est hors programme des classes préparatoires.



Une bijection de $[\![1,n-1]\!]$ dans $[\![1,n]\!]\setminus\{e\}$

Montrons que f est injective.

Soient m_1 et m_2 dans E tels que $f(m_1) = f(m_2)$.

Procédons par disjonction des cas.

- Si $m_1 < e$ et $m_2 < e$ alors $f(m_1) = m_1$ et $f(m_2) = m_2$ d'où $m_1 = m_2$.
- Si $m_1 \geqslant e$ et $m_2 \geqslant e$ alors $f(m_1) = m_1 + 1$ et $f(m_2) = m_2 + 1$ d'où $m_1 + 1 = m_2 + 1$ et en conséquence $m_1 = m_2$.
- Si $m_1 < e$ et $m_2 \geqslant e$ alors $f(m_1) = m_1 < e$ et $f(m_2) = m_2 + 1 > e$, ce cas ne peut se produire puisqu'on a supposé $f(m_1) = f(m_2)$.
- Si $m_1 \geqslant e$ et $m_2 < e$ alors $f(m_1) = m_1 + 1 > e$ et $f(m_2) = m_2 < e$, ce cas ne peut se produire non plus.

Dans tous les cas envisageables on a $m_1 = m_2$ donc f est injective.

Montrons que f est surjective.

Soit $m \in F$. Trouvons-lui un antécédent.

- Si $m < e$ alors m lui-même convient puisque dans ce cas $f(m) = m$.
- Si $m > e$ alors $m - 1 \geqslant e$ convient puisque dans ce cas $f(m-1) = (m-1)+1 = m$.

Tout élément de F admet un antécédent dans E par f ce qui prouve la surjectivité.

En conclusion f est bijective d'où le lemme.

Remarque

Le lemme ci-dessus reste encore valable si $n = 1$ car, dans ce cas, la question est de savoir si une application f de $\varnothing$ dans $\varnothing$ est bijective et la réponse est affirmative ! En effet, existe-t-il des éléments x_1 et x_2 distincts de l'ensemble de départ ayant même image ? Non, donc on ne peut pas dire que f n'est pas injective. Existe-t-il des éléments dans l'ensemble d'arrivée sans antécédent ? Non, donc on ne peut pas dire que f n'est pas surjective. Donc f est bien bijective.

Une première application de ce lemme est le corollaire suivant.

Corollaire 2

Pour toute partie A de $[\![1\,,n]\!]$, il existe une bijection de A sur $[\![1\,,m]\!]$ où $m \in [\![1\,,n]\!]$.

Ce corollaire permettra de démontrer un peu plus loin que toute partie d'un ensemble fini est également finie.

Demonstration

On pourrait faire une démonstration par récurrence sur n mais on peut être plus efficace en utilisant le lemme précédent. Considérons l'ensemble K des entiers naturels k pour lesquels il existe une injection de A dans $[\![1\,,k]\!]$:

$$K = \{k \in \mathbb{N} \mid \exists f : A \longrightarrow [\![1\,,k]\!] \text{ injective}\}$$

Cet ensemble est une partie de $\mathbb{N}$ qui est **non vide** puisque qu'elle contient l'entier n. En effet, l'application de A dans $[\![1\,,n]\!]$ qui à tout élément de A s'associe à lui-même[44] est injective. D'après l'axiome 1, page 35 l'ensemble K admet donc un plus petit élément m (et on a $1 \leqslant m \leqslant n$). Ainsi, il existe une injection f de A dans $[\![1\,,m]\!]$.
Supposons un instant que f ne soit pas surjective, alors il existerait un élément $e \in [\![1\,,m]\!]$ tel que $e \notin f(A)$. On peut alors considérer l'application $\tilde{f}$ définie par :

$$\begin{array}{rccc} \tilde{f}: & A & \longrightarrow & [\![1\,,m]\!] \setminus \{e\} \\ & x & \longmapsto & f(x) \end{array}$$

Cette application $\tilde{f}$ est toujours injective (puisque f l'est).
Par ailleurs, d'après le lemme 1, il existe une bijection g entre $[\![1\,,m]\!] \setminus \{e\}$ et $[\![1\,,m-1]\!]$.
Ainsi, la composée $g \circ \tilde{f}$ serait une injection de A dans $[\![1\,,m-1]\!]$ ce qui contredirait la minimalité de m. En conclusion f est surjective, donc bijective.

Poursuivons avec un second lemme très utile...

Lemme 2

Soient n et m deux entiers naturels non nuls.

S'il existe une injection f de $[\![1\,,n]\!]$ dans $[\![1\,,m]\!]$ alors $n \leqslant m$.

44. Si $A \subseteq B$, alors l'application :

$$\begin{array}{rccc} i: & A & \longrightarrow & B \\ & x & \longmapsto & x \end{array}$$

s'appelle une *injection canonique*. C'est clairement une injection, car $i(x_1) = i(x_2) \implies x_1 = x_2$. De plus, on a $i(A) = A$.

Index

D

E

S

T

U

V

W

Y

Z